aws

Guía para desarrolladores

AWS WAF, AWS Firewall Manager, y AWS Shield Advanced

AWS WAF, AWS Firewall Manager, y AWS Shield Advanced: Guía para desarrolladores

Table of Contents

¿Qué son AWS WAF, AWS Shield Advanced; y AWS Firewall Manager?

Pueden usar AWS WAFAWS Shield, y AWS Firewall Manager juntos para crear una solución de seguridad integral. AWS WAF es un firewall de aplicaciones web que puede utilizar para supervisar las solicitudes web que los usuarios finales envían a sus aplicaciones y para controlar el acceso a su contenido. Shield Advanced proporciona protección contra los ataques de denegación de servicio distribuido (DDoS) a AWS los recursos, en las capas de red y transporte (capas 3 y 4) y en la capa de aplicaciones (capa 7). AWS Firewall Manager proporciona administración de protecciones como AWS WAF Shield Advanced en todas las cuentas y los recursos, incluso cuando se agregan nuevos recursos.

Temas

¿Qué es AWS WAF?

AWS WAF es un firewall de aplicaciones web que le permite supervisar las solicitudes HTTP y HTTPS que se reenvían a los recursos de sus aplicaciones web protegidas. Puede proteger los siguientes tipos de recursos:

- CloudFront Distribución en Amazon
- API de REST de Amazon API Gateway
- Equilibrador de carga de aplicación
- AWS AppSync API GraphQL
- Grupo de usuarios de Amazon Cognito
- AWS App Runner servicio
- AWS Instancia de acceso verificado

AWS WAF le permite controlar el acceso a su contenido. En función de las condiciones que especifique, como las direcciones IP de las que provienen las solicitudes o los valores de las

cadenas de consulta, su recurso protegido responde a las solicitudes con el contenido solicitado, con un código de estado HTTP 403 (Prohibido) o con una respuesta personalizada.

En el nivel más simple, AWS WAF le permite elegir uno de los siguientes comportamientos:

- Permita todas las solicitudes excepto las que especifique: esto resulta útil si desea que Amazon CloudFront, Amazon API Gateway, Application Load Balancer AWS AppSync, Amazon Cognito AWS App Runner AWS o Verified Access sirvan contenido para un sitio web público, pero también desea bloquear las solicitudes de los atacantes.
- Bloquear todas las solicitudes, excepto las que especifique: esto es útil si quiere distribuir contenido a un sitio web restringido cuyos usuarios se puedan identificar fácilmente por medio de propiedades de las solicitudes web, como las direcciones IP que utilizan para navegar en el sitio web.
- Contar las solicitudes que coincidan con sus criterios: puede utilizar la acción Count para hacer un seguimiento de su tráfico web sin modificar la forma en que lo administra. Puede utilizarla para una supervisión general y también para probar sus nuevas reglas de manejo de solicitudes web. Si quiere permitir o bloquear las solicitudes en función de las nuevas propiedades de las solicitudes web, primero puede configurarlas AWS WAF para que cuenten las solicitudes que coincidan con esas propiedades. Esto le permite confirmar sus nuevos ajustes de configuración antes de cambiar las reglas para permitir o bloquear solicitudes coincidentes.
- Ejecutar CAPTCHA o comprobaciones de desafío frente a solicitudes que coincidan con sus criterios: puede implementar CAPTCHA y controles de desafío silenciosos frente a solicitudes para ayudar a reducir el tráfico de bots a sus recursos protegidos.

Su uso AWS WAF tiene varias ventajas:

- Protección adicional frente a ataques web gracias al uso de criterios especificados. Puede definir los criterios usando características de solicitudes web, como las siguientes:
  - Direcciones IP de origen de las solicitudes.
  - País de origen de las solicitudes.
  - Valores indicados en los encabezados de solicitudes.
  - Cadenas que aparecen en las solicitudes, ya sean cadenas específicas o cadenas que coinciden con patrones de expresiones regulares (regex).
  - Longitud de las solicitudes.

  - Presencia de código SQL que probablemente sea malintencionado (conocido como inyección de código SQL).
  - Presencia de un script que probablemente sea malintencionado (conocido como scripting entre sitios).
- Reglas que pueden permitir, bloquear o contar solicitudes web que cumplen los criterios especificados. Como alternativa, las reglas pueden bloquear o contar las solicitudes web que no solo cumplen los criterios especificados, sino que también superan un número específico de solicitudes en un minuto o cinco minutos.
- Reglas que pueda reutilizar para varias aplicaciones web.
- Gestioné grupos de reglas de AWS Marketplace vendedores AWS y vendedores.
- Métricas y solicitudes web muestreadas en tiempo real.
- Administración automatizada mediante la AWS WAF API.

Si desea un control detallado sobre la protección que agrega a sus recursos, AWS WAF por sí solo podría ser la elección correcta. Para obtener más información al respecto AWS WAF, consulteAWS WAF.

¿Qué es AWS Shield Advanced?

Puede utilizar listas de control de acceso AWS WAF web (ACL web) para minimizar los efectos de un ataque de denegación de servicio distribuido (DDoS). Para una protección adicional contra los ataques DDoS, AWS también ofrece y. AWS Shield Standard AWS Shield Advanced AWS Shield Standard se incluye automáticamente sin coste adicional más allá de lo que ya paga AWS WAF y de sus demás AWS servicios.

Shield Advanced ofrece una protección ampliada contra ataques DDoS para sus instancias de Amazon EC2, los balanceadores de carga de Elastic Load Balancing, las distribuciones CloudFront , las zonas alojadas de Route 53 y los aceleradores estándar. AWS Global Accelerator Shield Advanced conlleva cargos adicionales. Las opciones y características de Shield Advanced incluyen mitigación automática de DDoS en la capa de aplicación, visibilidad avanzada de eventos y soporte dedicado del equipo de respuesta de Shield (SRT). Si posee sitios web de alta visibilidad o sufre ataques DDoS frecuentes, debería plantearse comprar las protecciones adicionales que proporciona Shield Advanced. Para obtener más información, consulte AWS Shield Advanced capacidades y opciones y Decidir si desea suscribirse a protecciones adicionales AWS Shield Advanced y aplicarlas.

¿Qué es? AWS Firewall Manager

AWS Firewall Manager simplifica las tareas de administración y mantenimiento en varias cuentas y recursos para una variedad de protecciones AWS WAF, AWS Shield Advanced como los grupos de seguridad de Amazon VPC y las ACL de red AWS Network Firewall, y el firewall de DNS Amazon Route 53 Resolver. Con Firewall Manager, configure las protecciones una única vez y el servicio las aplica automáticamente en todas sus cuentas y recursos, incluso cuando se agreguen nuevas cuentas y recursos.

Para obtener más información sobre Firewall Manager, consulte AWS Firewall Manager.

Configuración de su cuenta para usar los servicios

En este tema se describen los pasos preliminares, como la creación de una cuenta, para prepararte para usarla AWS WAF AWS Firewall Manager, y AWS Shield Advanced. No se le cobrarán estos elementos preliminares. Solo se le cobrará por AWS los servicios que utilice.

Temas

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Signing in as the root user en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Descargar herramientas

AWS Management Console Incluye una consola para AWS WAF, y AWS Shield Advanced AWS Firewall Manager, pero si desea acceder a los servicios mediante programación, consulte lo siguiente:

- Las guías de la API documentan las operaciones que admiten los servicios y proporcionan enlaces a la documentación relacionada del SDK y la CLI:
  - AWS WAF Referencia de la API
  - AWS Shield Advanced Referencia de la API
  - AWS Firewall Manager Referencia de la API
- Para llamar a una API sin tener que gestionar detalles de bajo nivel, como el ensamblaje de solicitudes HTTP sin procesar, puedes usar un SDK. AWS Los AWS SDK proporcionan funciones y tipos de datos que encapsulan la funcionalidad de los servicios. AWS Para descargar un AWS SDK y acceder a las instrucciones de instalación, consulta la página correspondiente:
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

Para obtener una lista completa de AWS los SDK, consulte Herramientas para Amazon Web Services.

- Puede usar AWS Command Line Interface (AWS CLI) para controlar varios AWS servicios desde la línea de comandos. También puede automatizar los comandos utilizando scripts. Para obtener más información, consulte AWS Command Line Interface.
- AWS Tools for Windows PowerShell admite estos AWS servicios. Para obtener más información, consulte Referencia de cmdlet de AWS Tools for PowerShell.

AWS WAF

AWS WAF es un firewall de aplicaciones web que le permite supervisar las solicitudes HTTP (S) que se reenvían a los recursos de aplicaciones web protegidas. Puede proteger los siguientes tipos de recursos:

- CloudFront Distribución en Amazon
- API de REST de Amazon API Gateway
- Equilibrador de carga de aplicación
- AWS AppSync API GraphQL
- Grupo de usuarios de Amazon Cognito
- AWS App Runner servicio
- AWS Instancia de acceso verificado

AWS WAF le permite controlar el acceso a su contenido. En función de los criterios que especifique, como las direcciones IP de las que provienen las solicitudes o los valores de las cadenas de consulta, el servicio asociado a su recurso protegido responde a las solicitudes con el contenido solicitado, con un código de estado HTTP 403 (Prohibido) o con una respuesta personalizada.

> **Note**
>
> También puede usarlo AWS WAF para proteger sus aplicaciones alojadas en contenedores de Amazon Elastic Container Service (Amazon ECS). Amazon ECS es un servicio de administración de contenedores muy escalable y rápido que facilita la tarea de ejecutar, detener y administrar contenedores de Docker en un clúster. Para usar esta opción, debe configurar Amazon ECS para que utilice un Application Load Balancer que esté habilitado para AWS WAF enrutar y proteger el tráfico HTTP (S) de capa 7 entre las tareas de su servicio. Para obtener más información, consulte Equilibrio de carga de servicio en la Guía para desarrolladores de Amazon Elastic Container Service.

Temas

- AWS WAF grupos de reglas
- AWS WAF reglas
- Manejo de componentes de solicitudes sobredimensionadas en AWS WAF
- Coincidencia de patrones de expresiones regulares en AWS WAF
- Conjuntos de IP y conjuntos de patrones de expresiones regulares en AWS WAF
- Solicitudes web y respuestas personalizadas en AWS WAF
- AWS WAF etiquetas en las solicitudes web
- AWS WAF mitigación inteligente de amenazas
- Registro del tráfico de ACL AWS WAF web
- Probando y ajustando sus AWS WAF protecciones
- Cómo AWS WAF funciona con las CloudFront funciones de Amazon
- Seguridad en el uso del AWS WAF servicio
- AWS WAF cuotas
- Migración de sus recursos AWS WAF clásicos a AWS WAF

Cómo AWS WAF funciona

Se utiliza AWS WAF para controlar la forma en que los recursos protegidos responden a las solicitudes web HTTP (S). Para ello, defina una lista de control de acceso (ACL) web y, a continuación, asóciela a uno o más recursos de aplicaciones web que desee proteger. Los recursos asociados reenvían las solicitudes entrantes a la ACL web AWS WAF para que las inspeccione.

En la ACL web, se crean reglas para definir los patrones de tráfico que se deben buscar en las solicitudes y especificar las acciones que se deben tomar en caso de que coincidan con las solicitudes. Actualmente, las opciones son las siguientes:

- Permitir que las solicitudes vayan al recurso protegido para su procesamiento y respuesta.
- Bloquear las solicitudes.
- Contar las solicitudes.
- Realizar comprobaciones CAPTCHA o de desafíos para las solicitudes con el fin de verificar el uso estándar del navegador y que los usuarios son humanos.

AWS WAF componentes

Los siguientes son los componentes centrales de AWS WAF:

- ACL web: se utiliza una lista de control de acceso (ACL) web para proteger un conjunto de AWS recursos. Cree una ACL web y defina su estrategia de protección mediante la adición de reglas. Las reglas definen los criterios para inspeccionar las solicitudes web y especifican qué acción tomar con respecto a las solicitudes que coincidan con sus criterios. También se establece una acción predeterminada para la ACL web que indica si bloquear o permitir las solicitudes que las reglas aún no hayan bloqueado o permitido. Para obtener más información acerca de las ACL web, consulte AWS WAF listas de control de acceso web (ACL web).

  Una ACL web es un AWS WAF recurso.

- Reglas: cada regla contiene una instrucción que define los criterios de inspección y una acción que se debe realizar si una solicitud web cumple con los criterios. Cuando una solicitud web cumple los criterios, se produce una coincidencia. Puede configurar reglas para bloquear las solicitudes coincidentes, permitirlas pasar, contarlas o ejecutar controles de bots con respecto a ellas mediante rompecabezas de CAPTCHA o desafíos silenciosos al navegador del cliente. Para obtener más información acerca de las reglas, consulte AWS WAF reglas.

  Una regla no es un AWS WAF recurso. Solamente existe en el contexto de una ACL web o un grupo de reglas.

- Grupos de reglas: puede definir reglas directamente dentro de una ACL web o en grupos de reglas reutilizables. AWS Las reglas administradas y AWS Marketplace los vendedores proporcionan grupos de reglas administradas para su uso. También puede definir sus propios grupos de reglas. Para obtener más información acerca de los grupos de reglas, consulte AWS WAF grupos de reglas.

  Un grupo de reglas es un AWS WAF recurso.

Temas

AWS WAF unidades de capacidad ACL web (WCU)

AWS WAF utiliza las unidades de capacidad de las ACL web (WCU) para calcular y controlar los recursos operativos necesarios para ejecutar las reglas, los grupos de reglas y las ACL web. AWS

WAF impone los límites de la WCU al configurar los grupos de reglas y las ACL web. Las WCU no afectan a la forma AWS WAF en que inspecciona el tráfico web.

AWS WAF gestiona la capacidad de las reglas, los grupos de reglas y las ACL web.

WCU de reglas

AWS WAF calcula la capacidad de las reglas al crear o actualizar una regla. AWS WAF calcula la capacidad de forma diferente para cada tipo de regla, a fin de reflejar el coste relativo de cada regla. Las reglas simples cuya ejecución supone un bajo coste utilizan menos WCU que las reglas más complejas que utilizan más potencia de procesamiento. Por ejemplo, una instrucción de regla de restricción de tamaño utiliza menos WCU que una instrucción que inspecciona las solicitudes mediante un conjunto de patrones de expresiones regex.

Los requisitos de capacidad de las reglas suelen empezar con un coste base para el tipo de regla y aumentan con la complejidad, por ejemplo, cuando se agregan transformaciones de texto antes de la inspección o si se inspecciona el cuerpo JSON. Para obtener información sobre los requisitos de capacidad de las reglas, consulte la lista de instrucciones de reglas en Conceptos básicos de las instrucciones de regla.

WCU de grupos de reglas

Los requisitos de WCU para un grupo de reglas vienen determinados por las reglas que defina dentro del grupo de reglas. La capacidad máxima de un grupo de reglas es de 5000 WCU.

Cada grupo de reglas tiene una configuración de capacidad inmutable, que el propietario asigna en el momento de la creación. Esto es válido para los grupos de reglas administrados y los grupos de reglas mediante los cuales se crean AWS WAF. Al modificar un grupo de reglas, los cambios deben mantener la WCU del grupo de reglas dentro de su capacidad. Esto garantiza que las ACL web que utilizan el grupo de reglas permanezcan dentro de sus requisitos de capacidad.

Las WCU que se utilizan en un grupo de reglas son la suma de las WCU de las reglas menos las optimizaciones de procesamiento que AWS WAF se puedan obtener al combinar el comportamiento de las reglas. Por ejemplo, si define dos reglas para examinar el mismo componente de solicitud web y cada una de las reglas aplica una transformación concreta al componente antes de inspeccionarlo, es posible que solo AWS WAF pueda cobrarle una vez por aplicar la transformación. El coste de la WCU para usar un grupo de reglas en una ACL web es siempre la configuración fija de la WCU que se definió al crear el grupo de reglas.

Al crear un grupo de reglas, asegúrese de establecer una capacidad lo suficientemente alta como para dar cabida a las reglas que quiera utilizar durante toda la vida útil del grupo de reglas.

WCU de la ACL web

Los requisitos de la WCU para una ACL web vienen determinados por las reglas y los grupos de reglas que utilice dentro de la ACL web.

- El coste de usar un grupo de reglas en una ACL web es la configuración de la capacidad del grupo de reglas.
- El costo de usar una regla es la WCU calculada por la regla menos cualquier optimización de procesamiento que AWS WAF se pueda obtener de la combinación de reglas de la ACL web. Por ejemplo, si define dos reglas para examinar el mismo componente de solicitud web y cada una de las reglas aplica una transformación concreta al componente antes de inspeccionarlo, es posible que solo AWS WAF pueda cobrarle una vez por aplicar la transformación.

El precio básico de una ACL web incluye hasta 1500 WCU. El uso de más de 1500 WCU implica tarifas adicionales, según un modelo de precios escalonado. AWS WAF ajusta automáticamente los precios de la ACL web a medida que cambia el uso de las WCU de la ACL web. Para obtener más información sobre precios, consulte precios de AWS WAF.

La capacidad máxima de una ACL web es de 5000 WCU.

Determinar las WCU para un grupo de reglas o una ACL web

Como se ha indicado en las secciones anteriores, el total de las WCU utilizadas en un grupo de reglas o ACL web será igual o inferior a la suma de las WCU de todas las reglas definidas en el grupo de reglas o ACL web.

En la AWS WAF consola, puede ver la capacidad consumida al agregar reglas a su ACL web o grupo de reglas. La consola muestra las unidades de capacidad actuales utilizadas al agregar las reglas.

A través de la API puede comprobar los requisitos de capacidad máxima de las reglas que desee utilizar en una ACL web o en un grupo de reglas. Para ello, proporcione la lista de JSON de las reglas a la llamada de verificación de capacidad. Para obtener más información, consulte CheckCapacityla referencia de la API AWS WAF V2.

Recursos con los que puede protegerse AWS WAF

Puede usar una ACL AWS WAF web para proteger los tipos de recursos globales o regionales. Para ello, asocie la ACL web con los recursos que desea proteger. La ACL web y todos AWS WAF los recursos que utilice deben estar ubicados en la región en la que se encuentra el recurso asociado. Para CloudFront las distribuciones de Amazon, se establece en EE. UU. Este (Norte de Virginia).

CloudFront Distribuciones de Amazon

Puede asociar una ACL AWS WAF web a una CloudFront distribución mediante la AWS WAF consola o las API. También puede asociar una ACL web a una CloudFront distribución al crear o actualizar la propia distribución. Para configurar una asociación en AWS CloudFormation, debe usar la configuración CloudFront de distribución. Para obtener información sobre Amazon CloudFront, consulta Cómo AWS WAF controlar el acceso a tu contenido en la Guía para CloudFront desarrolladores de Amazon.

AWS WAF está disponible en todo el mundo para CloudFront distribuciones, pero debe utilizar la región EE.UU. Este (Norte de Virginia) para crear su ACL web y todos los recursos utilizados en la ACL web, como grupos de reglas, conjuntos de IP y conjuntos de patrones de expresiones regulares. Algunas interfaces ofrecen la opción de región «Global ()CloudFront». Elegir esta opción es lo mismo que elegir la región Este de EE. UU. (Norte de Virginia) o “us-east-1“.

Recursos regionales

Puede proteger los recursos regionales en todas las regiones donde AWS WAF estén disponibles. Puede ver la lista en puntos de conexión y las cuotas AWS WAF en Referencia general de Amazon Web Services.

Puede utilizarlos AWS WAF para proteger los siguientes tipos de recursos regionales:

- API de REST de Amazon API Gateway
- Equilibrador de carga de aplicación
- AWS AppSync API GraphQL
- Grupo de usuarios de Amazon Cognito
- AWS App Runner servicio
- AWS Instancia de acceso verificado

Solamente puede asociar una ACL web a un equilibrador de carga de aplicación que se encuentre en Regiones de AWS. Por ejemplo, solamente puede asociar una ACL web a un equilibrador de carga de aplicación que se encuentre en AWS Outposts.

La ACL web y cualquier otro AWS WAF recurso que utilice deben estar ubicados en la misma región que los recursos protegidos. Al monitorear y administrar las solicitudes web de un recurso regional protegido, AWS WAF mantiene todos los datos en la misma región que el recurso protegido.

Restricciones a varias asociaciones de recursos

Puede asociar una única ACL web a uno o más AWS recursos, con las siguientes restricciones:

- Puede asociar cada AWS recurso a una sola ACL web. La relación entre la ACL web y AWS los recursos es one-to-many.
- Puede asociar una ACL web a una o más CloudFront distribuciones. No puede asociar una ACL web que haya asociado a una CloudFront distribución con ningún otro tipo de AWS recurso.

Empezar con AWS WAF

En este tutorial se muestra cómo utilizar AWS WAF para realizar las siguientes tareas:

- Configurar AWS WAF.
- Cree una lista de control de acceso web (ACL web) mediante el asistente de la AWS WAF consola.
- Elija los AWS recursos para los que desee AWS WAF inspeccionar las solicitudes web. En este tutorial se explican los pasos para Amazon CloudFront. El proceso es básicamente el mismo para una API REST de Amazon API Gateway, un Application Load Balancer, una API de AWS AppSync GraphQL, un grupo de usuarios de Amazon Cognito, un AWS App Runner servicio o una instancia de Verified Access. AWS
- Añada las reglas y los grupos de reglas que desea utilizar para filtrar las solicitudes web. Por ejemplo, puede especificar las direcciones IP de donde provienen las solicitudes y especificar valores incluidos en la solicitud que solo utilicen los atacantes. Especifique cómo administrar las solicitudes web coincidentes para cada regla. Puede hacer cosas como bloquearlas o contarlas, y puede ejecutar desafíos de bots como CAPTCHA. Defina una acción para cada regla que defina dentro de una ACL web y para cada regla que defina dentro de un grupo de reglas.
- Especifique una acción predeterminada para la ACL web, ya sea Block o Allow. Esta es la acción que AWS WAF se lleva a cabo en respuesta a una solicitud cuando las reglas de la ACL web no la permiten ni bloquean de forma explícita.

> **Note**
>
> AWS normalmente te factura menos de 0,25 USD al día por los recursos que crees durante este tutorial. Cuando haya completado el tutorial, le recomendamos que elimine los recursos para evitar incurrir en gastos innecesarios.

Temas

Paso 1: configurar AWS WAF

Si aún no ha seguido los pasos de configuración generales de Configuración de su cuenta para usar los servicios, hágalo ahora.

Paso 2: Crear una ACL web

La AWS WAF consola lo guía a través del proceso de configuración AWS WAF para bloquear o permitir las solicitudes web en función de los criterios que especifique, como las direcciones IP de las que se originan las solicitudes o los valores de las solicitudes. En este paso, va a crear una ACL web. Para obtener más información sobre las ACL AWS WAF web, consulteAWS WAF listas de control de acceso web (ACL web).

Para crear una ACL web

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.
2. En la página de AWS WAF inicio, selecciona Crear ACL web.
3. En Name (Nombre), escriba el nombre que desea utilizar para identificar esta ACL web.

   > **Note**
   >
   > No se puede cambiar el nombre después de crear la ACL web.

4. (Opcional) En Description - optional (Descripción: opcional), introduzca una descripción más larga para la ACL web si lo desea.
5. Para el nombre de la CloudWatch métrica, cambie el nombre predeterminado, si corresponde. Siga las instrucciones de la consola para ver los caracteres válidos. El nombre no puede

contener caracteres especiales, espacios en blanco ni se pueden utilizar nombres de métricas reservados para AWS WAF, como "All" y "Default_Action".

> **Note**
>
> No puede cambiar el nombre de la CloudWatch métrica después de crear la ACL web.

6. En Tipo de recurso, elija CloudFrontdistribuciones. La región se rellena automáticamente como Global (CloudFront) para CloudFront las distribuciones.
7. (Opcional) En AWS Recursos asociados (opcional), elija Agregar AWS recursos. En el cuadro de diálogo, elija los recursos que desea asociar y, a continuación, elija Agregar. AWS WAF le devuelve a la página Describir la ACL web y los recursos asociados de AWS .
8. Elija Siguiente.

Paso 3: Agregar una regla de coincidencia de cadena

En este paso, creará una regla con una declaración de coincidencia de cadena e indicará qué hacer con las solicitudes que coinciden. Una instrucción de regla de coincidencia de cadena identifica las cadenas que desea que AWS WAF busque en una solicitud. Normalmente, una cadena se compone de caracteres ASCII imprimibles, pero puede especificar cualquier carácter comprendido entre los valores hexadecimales 0x00 y 0xFF (valores decimales 0 a 255). Además de especificar la cadena que se va a buscar, se especifica el componente de la solicitud web en el que se desea buscar, como un encabezado, una cadena de consulta o el cuerpo de la solicitud.

Este tipo de instrucción funciona en un componente de solicitud web y requiere la siguiente configuración del componente de la solicitud:

- Componente de solicitud: la parte de la solicitud web que se va a inspeccionar, por ejemplo, una cadena de consulta o el cuerpo.

> **Warning**
>
> Si inspeccionas el cuerpo, el cuerpo de JSON, los encabezados o las cookies de los componentes de la solicitud, consulta las limitaciones en cuanto a la cantidad de contenido que AWS WAF se puede inspeccionar. Manejo de componentes de solicitudes sobredimensionadas en AWS WAF

Para obtener información sobre los componentes de la solicitud web, consulte Especificación y manejo de componentes de solicitudes web.

- Transformaciones de texto opcionales: transformaciones que desea AWS WAF realizar en el componente de la solicitud antes de inspeccionarlo. Por ejemplo, puede convertir a minúsculas o normalizar el espacio en blanco. Si especifica más de una transformación, las AWS WAF procesa en el orden indicado. Para obtener más información, consulte Opciones de transformación de texto.

Para obtener información adicional sobre AWS WAF las reglas, consulteAWS WAF reglas.

Para crear una declaración de regla de coincidencia de cadena

1. En la página Add rules and rule groups (Añadir reglas y grupos de reglas), elija Add rules (Añadir reglas), Add my own rules and rule groups (Añadir mis propias reglas y grupos de reglas), Rule builder (Generador de reglas) y, a continuación, Rule visual editor (Editor visual de reglas).

   > **Note**
   >
   > La consola proporciona Rule visual editor (Editor visual de reglas) y también Rule JSON editor (Editor JSON de reglas). El editor JSON facilita la copia de configuraciones entre ACL web y es necesario para conjuntos de reglas más complejos, como los que cuentan con múltiples niveles de anidamiento.
   > Este procedimiento utiliza Rule visual editor (Editor visual de reglas).

2. En Name (Nombre), introduzca el nombre que desea utilizar para identificar esta regla.
3. En Type (Tipo), elija Regular rule (Regla normal).
4. En If a request (Si una solicitud), elija matches the statement (coincide con la declaración).

   Las demás opciones son para los tipos de instrucciones de reglas lógicas. Puede utilizarlas para combinar o anular los resultados de otras instrucciones de reglas.
5. En Statement, en Inspect, abra el menú desplegable y elija el componente de solicitud web que desee AWS WAF inspeccionar. En este ejemplo, seleccione Header.

   Al elegir Header (Encabezado), también debe especificar qué encabezado desea que AWS WAF inspeccione. Escriba **`User-Agent`**. Este valor no distingue entre mayúsculas y minúsculas.

6. En Match type (Tipo de coincidencia), decida si la cadena especificada tiene que aparecer en el encabezado `User-Agent`.

   En este ejemplo, elija Exactly matches string (Coincide exactamente con la cadena). Esto indica que AWS WAF inspecciona el encabezado del agente de usuario de cada solicitud web en busca de una cadena que sea idéntica a la cadena que especifiques.

7. En String to match (Cadena que debe coincidir), especifique la cadena que quiere que AWS WAF busque. La longitud máxima de String to match (Cadena que debe coincidir) es de 200 caracteres. Si desea especificar un valor con codificación base64, puede especificar hasta 200 caracteres antes de la codificación.

   Para este ejemplo, introduzca. MyAgent AWS WAF inspeccionará el `User-Agent` encabezado de las solicitudes web en busca del valor`MyAgent`.

8. Deje el campo Text transformation (Transformación de texto) establecido en None (Ninguna).

9. En Acción, seleccione la acción que desea que realice la regla cuando coincida con una solicitud web. Para este ejemplo, elija Recuento y deje las demás opciones como están. La acción de recuento crea métricas para las solicitudes web que coincidan con la regla, pero no afecta a si la solicitud está permitida o bloqueada. Para obtener más información sobre estas opciones, consulte Acción de regla y Evaluación de reglas y grupos de reglas de ACL web.

10. Seleccione Añadir regla.

Paso 4: Añadir un grupo de reglas de reglas AWS gestionadas

AWS Managed Rules ofrece un conjunto de grupos de reglas administradas para su uso, la mayoría de los cuales son gratuitos para AWS WAF los clientes. Para obtener más información acerca de los grupos de reglas, consulte AWS WAF grupos de reglas. Agregaremos un grupo de reglas AWS administradas a esta ACL web.

Para agregar un grupo de reglas de reglas AWS administradas

1. En la página Add rules and rule groups (Añadir reglas y grupos de reglas), elija Add rules (Añadir reglas) y, a continuación, Add managed rule groups (Añadir grupos de reglas administrados).

2. En la página Agregar grupos de reglas administrados, amplíe la descripción de los grupos de reglas administrados de AWS . (También verás los anuncios que se ofrecen a los AWS Marketplace vendedores. Puedes suscribirte a sus ofertas y luego utilizarlas de la misma manera que para los grupos de reglas de AWS Managed Rules).

3. Realice lo siguiente para cada grupo de reglas que desee agregar:

   a. En la columna Acción, active la opción Agregar a la ACL web.

   b. Seleccione Editar y, en la descripción de Reglas del grupo de reglas, abra el menú desplegable Anular todas las acciones de reglas y seleccione Count. Se establece que la acción de todas las reglas del grupo de reglas es solo contar. Esto le permite ver cómo se comportan todas las reglas del grupo de reglas con sus solicitudes web antes de usarlas.

   c. Seleccione Guardar reglas.

4. En la página Agregar grupos de reglas administrados, elija Agregar reglas. De este modo, volverá a la página Añadir reglas y grupos de reglas.

Paso 5: Finalizar la configuración de ACL web

Cuando haya terminado de añadir reglas y grupos de reglas a la configuración de ACL web, puede terminarla. Para ello, administre la prioridad de las reglas en la ACL web y configure parámetros como métricas, etiquetado y registro.

Para finalizar la configuración de ACL web:

1. En la página Add rules and rule groups (Añadir reglas y grupos de reglas), elija Next (Siguiente).
2. En la página Definir la prioridad de las reglas, puede ver el orden de procesamiento de las reglas y los grupos de reglas en la ACL web. AWS WAF las procesa empezando por la parte superior de la lista. Para cambiar el orden de procesamiento, mueva las reglas hacia arriba o hacia abajo. Para ello, seleccione un elemento de la lista y elija Move up (Subir) o Move down (Bajar). Para obtener más información acerca de la prioridad de regla, consulte Procesamiento del orden de las reglas y los grupos de reglas en una ACL web.
3. Elija Siguiente.
4. En la página Configurar métricas, para CloudWatchlas métricas de Amazon, puedes ver las métricas planificadas para tus reglas y grupos de reglas y puedes ver las opciones de muestreo de solicitudes web. Para obtener información sobre cómo ver las solicitudes muestreadas, consulte Visualizar una muestra de solicitudes web. Para obtener información sobre CloudWatch las métricas de Amazon, consultaMonitorización con Amazon CloudWatch.

   Puede acceder a los resúmenes de las métricas de tráfico web en la página de la ACL web de la AWS WAF consola, en la pestaña Resumen del tráfico. Los paneles de la consola proporcionan

resúmenes casi en tiempo real de las métricas de Amazon CloudWatch de la ACL web. Para obtener más información, consulte Paneles de información general sobre el tráfico de ACL web.

5. Seleccione Siguiente.
6. En la página Review and create web ACL (Revisar y crear ACL web), revise la configuración y, a continuación, elija Create web ACL (Crear ACL web).

El asistente le devuelve a la página de Web ACL (ACL web), donde aparece la nueva ACL Web.

Paso 6: Eliminar los recursos

Acaba de completar correctamente el tutorial. Para evitar que tu cuenta acumule AWS WAF cargos adicionales, limpia los AWS WAF objetos que has creado. Como alternativa, puedes cambiar la configuración para que coincida con las solicitudes web que realmente deseas gestionar. AWS WAF

> **Note**
>
> AWS normalmente te factura menos de 0,25 USD al día por los recursos que crees durante este tutorial. Cuando haya acabado, le recomendamos que elimine los recursos para evitar incurrir en gastos innecesarios.

Para eliminar los objetos por los que se AWS WAF cobra

1. En la página Web ACL (ACL web), seleccione su ACL web de la lista y elija Edit (Editar).
2. En la pestaña AWS Recursos asociados, para cada recurso asociado, seleccione el botón de radio situado junto al nombre del recurso y, a continuación, elija Desasociar. Esto disocia la ACL web de sus recursos. AWS
3. En cada una de las pantallas siguientes, elija Next (Siguiente) hasta que vuelva a la página Web ACL (ACL web).

   En la página Web ACL (ACL web), seleccione su ACL web de la lista y elija Delete (Eliminar).

Las reglas y las declaraciones de reglas no existen fuera de las definiciones de ACL web y los grupos de reglas. Si elimina una ACL web, se eliminarán todas las reglas individuales que haya definido en la ACL web. Cuando elimina un grupo de reglas de una ACL web, simplemente se elimina la referencia.

AWS WAF listas de control de acceso web (ACL web)

Una lista de control de acceso web (ACL web) le proporciona un control detallado de todas las solicitudes web HTTP(S) a las que responde su recurso protegido. Puede proteger los recursos de Amazon CloudFront, Amazon API Gateway, Application Load Balancer AWS AppSync, Amazon Cognito AWS y AWS App Runner Verified Access.

Puede utilizar criterios como los siguientes para permitir o bloquear solicitudes:

- Origen de la dirección IP de la solicitud
- País de origen de la solicitud
- Coincidencia de cadena o expresión regular (regex) en una parte de la solicitud
- Tamaño de una parte determinada de la solicitud
- Detección de código SQL o secuencias de comandos malintencionados

También puede probar cualquier combinación de estas condiciones. Puede bloquear o contar las solicitudes web que no solo cumplan las condiciones especificadas, sino que también superen un número específico de solicitudes en un solo minuto. Puede combinar condiciones mediante el uso de operadores lógicos. También puede ejecutar rompecabezas de CAPTCHA y desafíos silenciosos a las sesiones de los clientes para las solicitudes.

En las declaraciones de AWS WAF reglas, debe indicar los criterios de coincidencia y la acción que se debe realizar en caso de que se produzcan coincidencias. Puede definir las instrucciones de las reglas directamente en su ACL web y en los grupos de reglas reutilizables que utilice en su ACL web. Para obtener una lista completa de opciones, consulte Conceptos básicos de las instrucciones de regla y Acción de regla.

Para especificar los criterios de inspección y gestión de las solicitudes web, lleve a cabo las siguientes tareas:

1. Elija la acción por defecto de ACL web para permitir Allow o bloquear Block solicitudes web que no coincidan con ninguna de las reglas que se han especificado. Para obtener más información, consulte La acción predeterminada de ACL web.
2. Agregue los grupos de reglas que desee utilizar en la ACL web. Los grupos de reglas administrados suelen contener reglas que bloquean las solicitudes web. Para obtener información acerca de los grupos de reglas, consulte AWS WAF grupos de reglas.

3. Especifique criterios de concordancia e instrucciones de tratamiento adicionales en una o varias reglas. Para agregar más de una regla, comience con las instrucciones de regla `AND` o `OR` y anide las reglas que desee combinar. Si desea negar una opción de regla, anide la regla en una instrucción NOT. Opcionalmente, puede utilizar una regla basada en frecuencia en lugar de una regla normal para limitar el número de solicitudes desde cualquier dirección IP que cumpla las condiciones. Para obtener más información acerca de las reglas, consulte AWS WAF reglas.

Si agrega más de una regla a una ACL web, AWS WAF evalúa las reglas en el orden en que aparecen en la ACL web. Para obtener más información, consulte Evaluación de reglas y grupos de reglas de ACL web.

Cuando se crea una ACL web, se especifican los tipos de recursos con los que se desea utilizar. Para obtener más información, consulte Crear una ACL web. Después de definir una ACL web, puede asociarla con sus recursos para comenzar a proporcionarles protección. Para obtener más información, consulte Asociar o desasociar una ACL web a un recurso AWS.

Cómo gestionan AWS los recursos los retrasos en las respuestas desde AWS WAF

En algunas ocasiones, AWS WAF puede producirse un error interno que retrase la respuesta a AWS los recursos asociados a la hora de permitir o bloquear una solicitud. En esas ocasiones, CloudFront normalmente permite la solicitud o entrega el contenido, mientras que los servicios regionales suelen denegar la solicitud y no entregar el contenido.

Temas

- Evaluación de reglas y grupos de reglas de ACL web
- La acción predeterminada de ACL web
- Gestión de los límites de tamaño de la inspección corporal
- Configuraciones para CAPTCHA, desafío y tokens
- Trabajar con ACL web

Evaluación de reglas y grupos de reglas de ACL web

La forma en la que una ACL web gestione una solicitud web dependerá de lo siguiente:

- La configuración de prioridad numérica de las reglas en la ACL web y dentro de los grupos de reglas
- La configuración de la acción en las reglas y en la ACL web
- Cualquier anulación que repercuta en las reglas y en los grupos de reglas que agregue

Para obtener una lista de la configuración de las acciones de reglas, consulte Acción de regla.

Puede personalizar la gestión de solicitudes y respuestas en la configuración de la acción de su regla y en la configuración de acción predeterminada de ACL web. Para obtener más información, consulte Solicitudes web y respuestas personalizadas en AWS WAF.

Temas

- Procesamiento del orden de las reglas y los grupos de reglas en una ACL web
- Cómo AWS WAF gestiona las acciones de reglas y grupos de reglas en una ACL web
- Opciones de anulación de acciones para grupos de reglas

Procesamiento del orden de las reglas y los grupos de reglas en una ACL web

En una ACL web y dentro de cualquier grupo de reglas, el orden de evaluación de las reglas se determina mediante la configuración de la prioridad numérica. A cada regla de una ACL web debe asignarle una configuración de prioridad única dentro de esa ACL web y a cada regla de un grupo de reglas debe asignarle una configuración de prioridad única dentro de ese grupo de reglas.

> **Note**
>
> Cuando administra grupos de reglas y ACL web a través de la consola, le AWS WAF asigna una configuración de prioridad numérica única en función del orden de las reglas de la lista. AWS WAF asigna la prioridad numérica más baja a la regla en la parte superior de la lista y la prioridad numérica más alta a la regla en la parte inferior.

Al AWS WAF evaluar una ACL web o un grupo de reglas con respecto a una solicitud web, evalúa las reglas desde la configuración de prioridad numérica más baja hasta que encuentra una coincidencia que finalice la evaluación o agote todas las reglas.

Por ejemplo, supongamos que tiene las siguientes reglas y grupos de reglas en su ACL web, priorizados como se muestra:

- Regla 1: prioridad 0
- RuleGroupA: prioridad 100
  - Regla A1: prioridad 10 000
  - Regla A2: prioridad 20 000
- Regla 2: prioridad 200
- RuleGroupB: prioridad 300
  - Regla B1: prioridad 0
  - Regla B2: prioridad 1

AWS WAF evaluaría las reglas de esta ACL web en el siguiente orden:

- Rule1
- RuleGroupUna regla A1
- RuleGroupUna regla A2
- Rule2
- RuleGroupRegla B B1
- RuleGroupRegla B: B2

Cómo AWS WAF gestiona las acciones de reglas y grupos de reglas en una ACL web

Al configurar las reglas y los grupos de reglas, usted elige cómo AWS WAF quiere gestionar las solicitudes web coincidentes:

- Allow y Block son acciones de finalización; las acciones Allow y Block detienen todos los demás procesamientos de la ACL web en la solicitud web coincidente. Si una regla de una ACL web encuentra una coincidencia para una solicitud y la acción de la regla es Allow oBlock, esa coincidencia determina la disposición final de la solicitud web para la ACL web. AWS WAF no procesa ninguna otra regla de la ACL web que venga después de la coincidente. Esto se cumple en el caso de las reglas que agrega directamente a la ACL web y las reglas que se encuentran en un grupo de reglas añadido. Con la acción Block, el recurso protegido no recibe ni procesa la solicitud web.
- Count es una acción no terminal: cuando una regla con una acción de Count coincide con una solicitud, AWS WAF cuenta la solicitud y, a continuación, continúa procesando las siguientes reglas del conjunto de reglas de la ACL web.

- CAPTCHAy Challenge pueden ser acciones que no terminan o terminan: cuando una regla con una de estas acciones coincide con una solicitud, AWS WAF comprueba el estado de su token. Si la solicitud tiene un token válido, AWS WAF trata la coincidencia de forma similar a una Count coincidencia y, a continuación, continúa procesando las reglas siguientes del conjunto de reglas de ACL web. Si la solicitud no tiene un token válido, AWS WAF finaliza la evaluación y envía al cliente un acertijo de CAPTCHA o un desafío silencioso de sesión del cliente en segundo plano para que lo resuelva.

Si la evaluación de la regla no da lugar a ninguna acción de finalización, se AWS WAF aplica la acción predeterminada de la ACL web a la solicitud. Para obtener más información, consulte La acción predeterminada de ACL web.

En su ACL web, puede anular la configuración de acciones de reglas de un grupo de reglas y puede anular la acción que devuelve un grupo de reglas. Para obtener más información, consulte Opciones de anulación de acciones para grupos de reglas.

Interacción entre las acciones y la configuración de prioridades

Las acciones que AWS WAF se aplican a una solicitud web se ven afectadas por la configuración de prioridad numérica de las reglas de la ACL web. Por ejemplo, supongamos que su ACL web tiene una regla con una acción Allow y una prioridad numérica de 50, y otra regla con una acción Count y una prioridad numérica de 100. AWS WAF evalúa las reglas de una ACL web por orden de prioridad, empezando por la configuración más baja, por lo que evaluará la regla de permiso antes que la regla de recuento. Una solicitud web que cumpla ambas reglas coincidirá primero con la regla de permiso. Como Allow se trata de una acción de finalización, AWS WAF detendrá la evaluación en este momento y no evaluará la solicitud según la regla de recuento.

- Si solo quiere incluir las solicitudes que no coincidan con la regla de permiso en las métricas de las reglas de recuento, entonces, la configuración de prioridades de las reglas podría funcionar.
- Por otro lado, si quiere métricas de recuento de la regla de recuento incluso para las solicitudes que coincidan con la regla de permiso, tendrá que darle a la regla de recuento una prioridad numérica inferior a la de la regla de permiso, de modo que se ejecute primero.

Para obtener más información acerca de la configuración de prioridad, consulte Procesamiento del orden de las reglas y los grupos de reglas en una ACL web.

Opciones de anulación de acciones para grupos de reglas

Cuando agrega un grupo de reglas a su ACL web, puede anular las acciones que realiza cuando las solicitudes web coinciden. Si se anulan las acciones de un grupo de reglas en la configuración de la ACL web, no se altera el grupo de reglas en sí. Solo altera la forma en que se AWS WAF usa el grupo de reglas en el contexto de la ACL web.

La acción de la regla del grupo de reglas anula

Puede anular las acciones de las reglas dentro de un grupo de reglas para cualquier acción de regla válida. Al hacerlo, las solicitudes coincidentes se gestionan exactamente como si la acción de regla configurada fuera la configuración de anulación.

> **Note**
>
> Las acciones de la regla pueden ser de finalización o no. Una acción de finalización detiene la evaluación de la solicitud por parte de la ACL web y permite que continúe con la aplicación protegida o la bloquea.

Estas son las opciones de la acción de la regla:

- Allow— AWS WAF permite reenviar la solicitud al AWS recurso protegido para su procesamiento y respuesta. Se trata de una acción de finalización. En las reglas que defina, puede insertar encabezados personalizados en la solicitud antes de reenviarla al recurso protegido.
- Block— AWS WAF bloquea la solicitud. Se trata de una acción de finalización. De forma predeterminada, el AWS recurso protegido responde con un código de `403 (Forbidden)` estado HTTP. En las reglas que defina, puede personalizar la respuesta. Cuando AWS WAF bloquea una solicitud, la configuración de la Block acción determina la respuesta que el recurso protegido envía al cliente.
- Count— AWS WAF cuenta la solicitud pero no determina si se permite o se bloquea. Se trata de una acción no terminal. AWS WAF continúa procesando las reglas restantes en la ACL web. En las reglas que defina, puede insertar encabezados personalizados en la solicitud y puede agregar etiquetas con las que puedan coincidir otras reglas.
- CAPTCHAy Challenge: AWS WAF usa acertijos CAPTCHA y desafíos silenciosos para verificar que la solicitud no proviene de un bot, y AWS WAF usa fichas para rastrear las respuestas recientes de los clientes que han obtenido buenos resultados.

Los acertijos de CAPTCHA y los desafíos silenciosos solo se pueden ejecutar cuando los navegadores acceden a puntos finales HTTPS. Los clientes del navegador deben ejecutarse en contextos seguros para poder adquirir los tokens.

> **Note**
>
> Se le cobrarán tarifas adicionales cuando utilice la acción de regla CAPTCHA o Challenge en una de sus reglas o como anulación de una acción de regla en un grupo de reglas. Para obtener más información, consulte AWS WAF Precios.

Estas acciones de regla pueden ser de finalización o no, según el estado del token de la solicitud:

- No se cancela para un token válido y no caducado: si el token es válido y no ha caducado según el CAPTCHA configurado o el tiempo de inmunidad de impugnación, AWS WAF gestiona la solicitud de forma similar a la acción. Count AWS WAF continúa inspeccionando la solicitud web en función de las demás reglas de la ACL web. Al igual que en la configuración de Count, en las reglas que defina, puede configurar opcionalmente estas acciones con encabezados personalizados para insertarlos en la solicitud y puede agregar etiquetas con las que puedan coincidir otras reglas.
- Finalizar con una solicitud bloqueada de un token no válido o caducado: si el token no es válido o la marca de tiempo indicada ha caducado, AWS WAF finaliza la inspección de la solicitud web y bloquea la solicitud, de forma similar a la acción. Block AWS WAF luego responde al cliente con un código de respuesta personalizado. PuesCAPTCHA, si el contenido de la solicitud indica que el navegador del cliente puede gestionarla, AWS WAF envía un acertijo CAPTCHA en un JavaScript intersticial, diseñado para distinguir a los clientes humanos de los bots. Para elloChallenge, AWS WAF envía un JavaScript intersticial con un desafío silencioso diseñado para distinguir los navegadores normales de las sesiones ejecutadas por bots.

Para obtener información adicional, consulte CAPTCHAy Challenge en AWS WAF.

Para obtener información acerca de cómo utilizar esta acción, consulte Invalidar acciones de reglas en un grupo de reglas.

Anulación de la acción de regla para Count

El caso de uso más común para anular las acciones de reglas es anular algunas o todas las acciones de la regla para Count, con el fin de probar y supervisar el comportamiento de un grupo de reglas antes de ponerlo en producción.

También puede utilizar esto para solucionar problemas relacionados con un grupo de reglas que esté generando falsos positivos. Los falsos positivos se producen cuando un grupo de reglas bloquea el tráfico que no se espera que bloquee. Si identifica una regla dentro de un grupo de reglas que bloquee solicitudes que desea permitir, puede mantener la anulación de la acción de recuento en esa regla para evitar que actúe sobre sus solicitudes.

Para obtener más información acerca de cómo utilizar la anulación de la acción de las reglas en las pruebas, consulte Probando y ajustando sus AWS WAF protecciones.

Lista de JSON: **`RuleActionOverrides`** reemplaza a **`ExcludedRules`**

Si configuró las acciones de las reglas del grupo de reglas Count en su configuración de ACL web antes del 27 de octubre de 2022, AWS WAF guardó las anulaciones en la ACL web JSON como. `ExcludedRules` Ahora la configuración JSON para anular una regla en Count se encuentra en la configuración `RuleActionOverrides`.

Al utilizar la AWS WAF consola para editar la configuración del grupo de reglas existente, la consola convierte automáticamente cualquier `ExcludedRules` configuración del JSON en `RuleActionOverrides` configuración, con la acción de anulación establecida en. Count

- Ejemplo de configuración actual:

```
      "ManagedRuleGroupStatement": {
         "VendorName": "AWS",
         "Name": "AWSManagedRulesAdminProtectionRuleSet",
         "RuleActionOverrides": [
           {
             "Name": "AdminProtection_URIPATH",
             "ActionToUse": {
               "Count": {}
             }
           }
         ]
```

- Ejemplo de configuración anterior:

```
OLD SETTING
```

```
        "ManagedRuleGroupStatement": {
           "VendorName": "AWS",
           "Name": "AWSManagedRulesAdminProtectionRuleSet",
           "ExcludedRules": [
             {
               "Name": "AdminProtection_URIPATH"
             }
           ]
OLD SETTING
```

Le recomendamos que actualice todas las configuraciones de `ExcludedRules` de sus listas JSON a las configuraciones de `RuleActionOverrides` con la acción establecida en Count. La API acepta cualquier configuración, pero si solo utiliza la nueva configuración de `RuleActionOverrides`, conseguirá coherencia en sus listas JSON entre el trabajo de la consola y el de la API.

El grupo de reglas devuelve la acción de anulación a Count

Puede anular la acción que devuelve el grupo de reglas, configurándola en Count.

> **Note**
>
> Esta no es una buena opción para probar las reglas de un grupo de reglas, ya que no altera la forma en que AWS WAF se evalúa el propio grupo de reglas. Solo afecta a la forma en que se AWS WAF gestionan los resultados que se devuelven a la ACL web a partir de la evaluación del grupo de reglas. Si desea probar las reglas de un grupo de reglas, utilice la opción descrita en la sección anterior, La acción de la regla del grupo de reglas anula.

Al anular la acción del grupo de reglas paraCount, AWS WAF procesa la evaluación del grupo de reglas con normalidad.

Si ninguna regla del grupo de reglas coincide o si todas las reglas coincidentes tienen una acción Count, esta anulación no afecta al procesamiento del grupo de reglas ni a la ACL web.

La primera regla del grupo de reglas que coincide con una solicitud web y que tiene una acción de regla de finalización hace AWS WAF que deje de evaluar el grupo de reglas y devuelva el resultado de la acción de finalización al nivel de evaluación de la ACL web. En este punto, en la evaluación de la ACL web, esta anulación entra en vigor. AWS WAF anula la acción de finalización para que el

resultado de la evaluación del grupo de reglas sea solo una acción. Count AWS WAF a continuación, continúa procesando el resto de las reglas de la ACL web.

Para obtener información acerca de cómo utilizar esta acción, consulte Sustitución del resultado de la evaluación de un grupo de reglas por Count.

La acción predeterminada de ACL web

Al crear y configurar una ACL web, debe establecer la acción predeterminada de la ACL web. AWS WAF aplica esta acción a cualquier solicitud web que supere todas las evaluaciones de reglas de la ACL web sin que se le aplique una acción de finalización. Una acción de finalización detiene la evaluación de la solicitud por parte de la ACL web y permite que continúe con la aplicación protegida o la bloquea. Para obtener información sobre las acciones de las reglas, consulte Acción de regla.

La acción predeterminada de la ACL web debe determinar la disposición final de la solicitud web, por lo que se trata de una acción de finalización:

- Allow: si desea permitir que la mayoría de los usuarios pueda acceder a su sitio web, pero desea bloquear el acceso a atacantes cuyas solicitudes provienen de direcciones IP específicas o cuyas solicitudes parecen contener código SQL malicioso o valores específicos, elija Allow como la acción predeterminada. A continuación, cuando agregue reglas a su ACL web, añada reglas que identifiquen y bloqueen las solicitudes específicas que desea bloquear. Con esta acción puede insertar encabezados personalizados en la solicitud antes de reenviarla al recurso protegido.
- Block: si desea evitar que la mayoría de posibles usuarios acceda a su sitio web, pero desea permitir el acceso a los usuarios cuyas solicitudes provienen de direcciones IP específicas o cuyas solicitudes contienen valores específicos, elija Block como la acción predeterminada. A continuación, cuando agregue reglas a su ACL web, agregue reglas que identifiquen y permitan las solicitudes específicas que desea permitir. De forma predeterminada, para la Block acción, el AWS recurso responde con un código de `403 (Forbidden)` estado HTTP, pero puede personalizar la respuesta.

Para obtener información sobre cómo personalizar las solicitudes y las respuestas, consulte Solicitudes web y respuestas personalizadas en AWS WAF.

La configuración de sus propias reglas y grupos de reglas depende en parte de si desea permitir o bloquear la mayoría de las solicitudes web. Por ejemplo, si quiere permitir la mayoría de las solicitudes, tiene que configurar la acción predeterminada de la ACL web para que Allow y, a

continuación, agregar reglas que identifiquen las solicitudes web que desea bloquear, como las siguientes:

- Las solicitudes que provengan de direcciones IP que realizan un número excesivo de solicitudes
- Las solicitudes que proceden de países en los que no opera o que con frecuencia son origen de ataques
- Las solicitudes que incluyen valores falsos en el encabezado `User-agent`
- Las solicitudes que parecen incluir código SQL malicioso

Las reglas de los grupos de reglas administrados suelen utilizar la acción Block, pero no todas. Por ejemplo, algunas reglas que se utilizan para el control de bots utilizan la configuración de la acciones de CAPTCHA y Challenge. Para obtener información acerca de los grupos de reglas administrados, consulte Grupos de reglas administrados.

Gestión de los límites de tamaño de la inspección corporal

El límite de tamaño corporal para la inspección es el tamaño corporal máximo solicitado que AWS WAF se puede inspeccionar. Cuando el cuerpo de una solicitud web supera el límite, el servicio de alojamiento subyacente solo reenvía el contenido que se encuentra dentro del límite AWS WAF para su inspección.

- Para Application Load Balancer y AWS AppSync, el límite se ha fijado en 8 KB (8.192 bytes).
- Para CloudFront API Gateway, Amazon Cognito, App Runner y Verified Access, el límite predeterminado es de 16 KB (16 384 bytes) y puede aumentarlo para cualquiera de los tipos de recursos en incrementos de 16 KB, hasta 64 KB. Las opciones de configuración son 16 KB, 32 KB, 48 KB y 64 KB.

Gestión de cuerpos sobredimensionados

Si su tráfico web incluye cuerpos que superan el límite, se aplicará el tratamiento de sobredimensionamiento que haya configurado. Para obtener información sobre las opciones de gestión de tamaños excesivos, consulte. Manejo de componentes de solicitudes sobredimensionadas en AWS WAF

Consideraciones de precios para aumentar la fijación de límites

AWS WAF cobra una tarifa base por inspeccionar el tráfico que esté dentro del límite predeterminado para el tipo de recurso.

CloudFrontEn el caso de los recursos de API Gateway, Amazon Cognito, App Runner y Verified Access, si aumentas el límite establecido, el tráfico que AWS WAF se puede inspeccionar incluye el tamaño de las personas hasta el nuevo límite. Solo se le cobrará un cargo adicional por la inspección de las solicitudes que tengan un tamaño superior a los 16 KB predeterminados. Para obtener más información sobre los precios, consulte Precios de AWS WAF.

Opciones para modificar el límite de tamaño de la inspección corporal

Puede configurar el límite de tamaño de la inspección corporal para los CloudFront recursos de API Gateway, Amazon Cognito, App Runner o Verified Access.

Al crear o editar una ACL web, puede modificar los límites de tamaño de la inspección corporal en la configuración de la asociación de recursos. Para la API, consulte la configuración de asociación de la ACL web en AssociationConfig. Para la consola, consulte la configuración en la página en la que especifica los recursos asociados a la ACL web. Para obtener instrucciones sobre la configuración de la consola, consulte Trabajar con ACL web.

Configuraciones para CAPTCHA, desafío y tokens

Puede configurar opciones en su ACL web para las reglas que utilizan las acciones CAPTCHA o Challenge reglas y para los SDK de integración de aplicaciones que gestionan los desafíos silenciosos de los clientes en materia de protecciones gestionadas. AWS WAF

Estas características mitigan la actividad de los bots al desafiar a los usuarios finales con rompecabezas de CAPTCHA y al plantear a las sesiones de los clientes desafíos silenciosos. Cuando el cliente responde correctamente, AWS WAF proporciona un token para que lo utilice en su solicitud web, con una marca de tiempo con las últimas respuestas acertadas a rompecabezas y desafíos. Para obtener más información, consulte AWS WAF mitigación inteligente de amenazas.

En su configuración de ACL web, puede configurar la forma en que AWS WAF administra estos tokens:

- Tiempos de inmunidad de un CAPTCHA y un desafío: especifican durante cuánto tiempo sigue siendo válido una marca de tiempo de un CAPTCHA o desafío. La configuración de las ACL web la heredan todas las reglas que no tienen configuradas sus propios ajustes de tiempo de inmunidad, así como los SDK de integración de aplicaciones. Para obtener más información, consulte Caducidad de la marca de tiempo: tiempos de inmunidad AWS WAF simbólica.
- Dominios de token: de forma predeterminada, solo AWS WAF acepta los tokens del dominio del recurso al que está asociada la ACL web. Si configura una lista de dominios simbólicos, AWS

WAF acepta los tokens de todos los dominios de la lista y del dominio del recurso asociado. Para obtener más información, consulte AWS WAF Configuración de la lista de dominios del token ACL web.

Trabajar con ACL web

En esta sección se proporcionan los procedimientos para crear, administrar y usar las ACL web a través de la AWS consola.

Para cualquier ACL web que utilice, puede acceder a los resúmenes de las métricas de tráfico web en la página de la ACL web de la AWS WAF consola, en la pestaña Descripción general del tráfico. Los paneles de la consola proporcionan resúmenes casi en tiempo real de las CloudWatch métricas de Amazon que AWS WAF recopila cuando evalúa el tráfico web de tu aplicación. Para obtener más información acerca de los paneles, consulte Paneles de información general sobre el tráfico de ACL web. Para obtener información adicional sobre la supervisión del tráfico de la ACL web, consulte Monitorización y ajuste.

Riesgo de tráfico de producción

Antes de implementar cambios en su ACL web para el tráfico de producción, pruébelos y ajústelos en un entorno provisional o de pruebas hasta que se sienta cómodo con el posible impacto en el tráfico. A continuación, pruebe y ajuste las reglas actualizadas en el modo de recuento con el tráfico de producción antes de habilitarlas. Para obtener instrucciones, consulte Probando y ajustando sus AWS WAF protecciones.

Note

El uso de más de 1500 WCU en una ACL web conlleva costos superiores al precio de la ACL web básica. Para obtener más información, consulte AWS WAF unidades de capacidad ACL web (WCU) y Precios de AWS WAF.

Incoherencias temporales durante las actualizaciones

Al crear o cambiar una ACL web u otros AWS WAF recursos, los cambios tardan un poco en propagarse a todas las áreas donde se almacenan los recursos. El tiempo de propagación puede oscilar entre unos segundos y varios minutos.

A continuación, se proporcionan ejemplos de incoherencias temporales que podría notar durante la propagación de los cambios:

- Después de crear una ACL web, si intenta asociarla a un recurso, es posible que se produzca una excepción que indique que la ACL web no está disponible.
- Después de agregar un grupo de reglas a una ACL web, las nuevas reglas del grupo de reglas pueden estar en vigor en un área en la que se usa la ACL web y no en otra.
- Tras cambiar la configuración de una acción de regla, es posible que vea la acción anterior en algunos lugares y la acción nueva en otros.
- Después de agregar una dirección IP a un conjunto de IP que está en uso dentro de una regla de bloqueo, es posible que la nueva dirección se bloquee en un área, pero que se permita en otra.

Temas

Crear una ACL web

Para crear una nueva ACL web, utilice el asistente de creación de ACL web siguiendo el procedimiento de esta página.

> ⚠ Riesgo de tráfico de producción
>
> Antes de implementar cambios en su ACL web para el tráfico de producción, pruébelos y ajústelos en un entorno provisional o de pruebas hasta que se sienta cómodo con el posible impacto en el tráfico. A continuación, pruebe y ajuste las reglas actualizadas en el modo de recuento con el tráfico de producción antes de habilitarlas. Para obtener instrucciones, consulte Probando y ajustando sus AWS WAF protecciones.

> **Note**
>
> El uso de más de 1500 WCU en una ACL web conlleva costos superiores al precio de la ACL web básica. Para obtener más información, consulte AWS WAF unidades de capacidad ACL web (WCU) y Precios de AWS WAF.

Para crear una ACL web

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.
2. Elija Web ACLs (ACL web) en el panel de navegación y, a continuación, elija Create web ACL (Crear ACL web).
3. En Name (Nombre), escriba el nombre que desea utilizar para identificar esta ACL web.

   > **Note**
   >
   > No se puede cambiar el nombre después de crear la ACL web.

4. (Opcional) En Description - optional (Descripción: opcional), introduzca una descripción más larga para la ACL web si lo desea.
5. Para el nombre de la CloudWatch métrica, cambie el nombre predeterminado, si corresponde. Siga las instrucciones de la consola para ver los caracteres válidos. El nombre no puede contener caracteres especiales, espacios en blanco ni nombres de métricas reservados AWS WAF, como «All» y «Default_Action».

   > **Note**
   >
   > No puede cambiar el nombre de la CloudWatch métrica después de crear la ACL web.

6. En Tipo de recurso, elija la categoría de AWS recurso que desee asociar a esta ACL web, ya sea CloudFront distribuciones de Amazon o recursos regionales. Para obtener más información, consulte Asociar o desasociar una ACL web a un recurso AWS.
7. En el caso de la región, si ha elegido un tipo de recurso regional, elija la región en la que desee AWS WAF almacenar la ACL web.

Solo tiene que elegir esta opción para los tipos de recursos regionales. En el caso de CloudFront las distribuciones, la región está codificada como región EE. UU. Este (Virginia del Norte) `us-east-1`, en el caso de las aplicaciones globales (CloudFront).

8. (CloudFront, API Gateway, Amazon Cognito, App Runner y Verified Access) Para solicitudes web, límite de tamaño de inspección (opcional), si desea especificar un límite de tamaño de inspección corporal diferente, seleccione el límite. Inspeccionar un tamaño corporal superior al valor predeterminado de 16 KB puede conllevar costes adicionales. Para obtener más información acerca de esta opción, consulte Gestión de los límites de tamaño de la inspección corporal.
9. (Opcional) Para AWS los recursos asociados: opcional, si desea especificar sus recursos ahora, elija Agregar AWS recursos. En el cuadro de diálogo, elija los recursos que desee asociar y, a continuación, elija Agregar. AWS WAF le devuelve a la página Describa la ACL web y AWS los recursos asociados.
10. Elija Siguiente.
11. (Opcional) Si desea agregar grupos de reglas administrados, en la página Add rules and rule groups (Añadir reglas y grupos de reglas), seleccione Add rules (Añadir reglas) y, a continuación, haga clic en Add managed rule groups (Añadir grupos de reglas administrados). Realice lo siguiente para cada grupo de reglas administrado que desee agregar:

    a. En la página Añadir grupos de reglas gestionados, amplía el listado para AWS ver los grupos de reglas gestionados o el AWS Marketplace vendedor que elijas.

    b. En el grupo de reglas que desea agregar, en la columna Acción, active la opción Añadir a la ACL web.

    Para personalizar la forma en que su ACL web utiliza el grupo de reglas, seleccione Editar. A continuación se muestra la configuración de personalización común:

    - Anule las acciones de reglas para algunas o todas las reglas. Si no define una acción de anulación para una regla, la evaluación utiliza la acción de la regla que está definida dentro del grupo de reglas. Para obtener más información acerca de esta opción, consulte Opciones de anulación de acciones para grupos de reglas.
    - Reduzca el alcance de las solicitudes web que inspecciona el grupo de reglas agregando una instrucción de restricción de acceso. Para obtener más información acerca de esta opción, consulte Instrucciones de restricción de acceso.

- Algunos grupos de reglas administradas requieren que se proporcione una configuración adicional. Consulte la documentación de su proveedor de grupos de reglas administradas. Para obtener información específica sobre los grupos de reglas de reglas AWS administradas, consultaAWS Reglas administradas para AWS WAF.

Cuando haya terminado con la configuración, seleccione Guardar regla.

Seleccione Add rules (Añadir reglas) para terminar de agregar reglas administradas y volver a la página Add rules and rule groups (Añadir reglas y grupos de reglas).

12. (Opcional) Si desea agregar su propio grupo de reglas, en la página Add rules and rule groups (Añadir reglas y grupos de reglas), elija Add rules (Añadir reglas) y, a continuación, seleccione Add my own rules and rule groups (Añadir mis propias reglas y grupos de reglas). Realice lo siguiente para cada grupo de reglas que desee agregar:

    a. En la página Add my own rules and rule groups (Añadir mis propias reglas y grupos de reglas), elija Rule group (Grupo de reglas).

    b. En Nombre, introduzca el nombre que desee usar para la regla del grupo de reglas en esta ACL web. No utilice nombres que comiencen por `AWS`, `Shield`, `PreFM` o `PostFM`. Estas cadenas están reservadas o pueden causar confusión con los grupos de reglas que otros servicios administran para usted. Consulte Grupos de reglas proporcionados por otros servicios.

    c. Seleccione el grupo de reglas de la lista.

    > **Note**
    >
    > Si desea anular las acciones de las reglas de un grupo de reglas propio, guárdelo primero en la ACL web y, a continuación, edite la ACL web y la declaración de referencia del grupo de reglas en la lista de reglas de la ACL web. Puede sustituir las acciones de la regla por cualquier configuración de acción válida, del mismo modo que puede hacer con los grupos de reglas gestionados.

    d. Seleccione Añadir regla.

13. (Opcional) Si desea agregar su propia regla, en la página Add rules and rule groups (Añadir reglas y grupos de reglas), elija Add rules (Añadir reglas), Add my own rules and rule groups (Añadir mis propias reglas y grupos de reglas), Rule builder (Generador, de reglas) y, a continuación, Rule visual editor (Editor visual de reglas).

> **Note**
>
> El Rule visual editor (Editor visual de reglas) de la consola admite un nivel de anidamiento. Por ejemplo, puede utilizar una sola instrucción lógica `AND` o `OR` y anidar otro nivel de instrucciones en ella, pero no puede anidar instrucciones lógicas dentro de instrucciones lógicas. Para administrar instrucciones de regla más complejas, utilice el Rule JSON editor (Editor de JSON de reglas). Para obtener información sobre todas las opciones de reglas, consulte AWS WAF reglas.
> Este procedimiento abarca el Rule visual editor (Editor visual de reglas).

a. En Name (Nombre), introduzca el nombre que desea utilizar para identificar esta regla. No utilice nombres que comiencen por `AWS`, `Shield`, `PreFM` o `PostFM`. Estas cadenas están reservadas o pueden causar confusión con los grupos de reglas que otros servicios administran para usted.

b. Introduzca la definición de la regla en función de sus necesidades. Puede combinar reglas en instrucciones de reglas lógicas `AND` y `OR`. El asistente le guía a través de las opciones para cada regla según el contexto. Para obtener información sobre las opciones de reglas, consulte AWS WAF reglas.

c. En Action (Acción), seleccione la acción que desea que realice la regla cuando coincida con una solicitud web. Para obtener más información acerca de sus opciones, consulte Acción de regla y Evaluación de reglas y grupos de reglas de ACL web.

   Si utiliza la acción CAPTCHA o Challenge, ajuste la configuración del tiempo de inmunidad según sea necesario para la regla. Si no especifica la configuración, la regla la hereda de la ACL web. Para modificar la configuración del tiempo de inmunidad de la ACL web, edite la ACL web después de crearla. Para obtener más información sobre los tiempos de inmunidad, consulte Caducidad de la marca de tiempo: tiempos de inmunidad AWS WAF simbólica.

   > **Note**
   >
   > Se le cobrarán tarifas adicionales cuando utilice la acción de regla CAPTCHA o Challenge en una de sus reglas o como anulación de una acción de regla en un grupo de reglas. Para obtener más información, consulte AWS WAF Precios.

Si quiere personalizar la solicitud o la respuesta, elija las opciones correspondientes y complete los detalles de la personalización. Para obtener más información, consulte Solicitudes web y respuestas personalizadas en AWS WAF.

Si quiere que su regla añada etiquetas a las solicitudes web coincidentes, elija las opciones correspondientes y rellene los detalles de la etiqueta. Para obtener más información, consulte AWS WAF etiquetas en las solicitudes web.

d. Seleccione Añadir regla.

14. Elija la acción predeterminada para ACL web, cualquiera de Block o Allow. Esta es la acción que AWS WAF se lleva a cabo cuando las reglas de la ACL web no la permiten ni bloquean de forma explícita. Para obtener más información, consulte La acción predeterminada de ACL web.

    Si desea personalizar la acción predeterminada, elija las opciones correspondientes y rellene los detalles de su personalización. Para obtener más información, consulte Solicitudes web y respuestas personalizadas en AWS WAF.

15. Puede definir una lista de dominios de token para permitir el intercambio de tokens entre aplicaciones protegidas. Las Challenge acciones CAPTCHA y los SDK de integración de aplicaciones que se implementan cuando se utilizan los grupos de reglas de AWS Managed Rules para el control de fraudes, la prevención del AWS WAF fraude en la creación de cuentas (ACFP), el control del AWS WAF fraude, la prevención del robo de cuentas (ATP) y AWS WAF el control de bots.

    No se admiten sufijos públicos. Por ejemplo, no puede usar `gov.au` o `co.uk` como dominio de token.

    De forma predeterminada, solo AWS WAF acepta los tokens del dominio del recurso protegido. Si agrega dominios simbólicos a esta lista, AWS WAF acepta los tokens para todos los dominios de la lista y para el dominio del recurso asociado. Para obtener más información, consulte AWS WAF Configuración de la lista de dominios del token ACL web.

16. Seleccione Siguiente.

17. En la página Definir la prioridad de las reglas, seleccione y mueva las reglas y los grupos de reglas AWS WAF al orden en que desee procesarlos. AWS WAF procesa las reglas empezando por la parte superior de la lista. Al guardar la ACL web, AWS WAF asigna una configuración de prioridad numérica a las reglas en el orden en el que las haya colocado en la lista. Para obtener

más información, consulte Procesamiento del orden de las reglas y los grupos de reglas en una ACL web.

18. Seleccione Siguiente.
19. En la página Configurar métricas, revise las opciones y aplique las actualizaciones que necesite. Puede combinar métricas de varias fuentes proporcionándoles el mismo nombre de CloudWatch métrica.
20. Elija Siguiente.
21. Revise las definiciones en la página Review and create web ACL (Revisar y crear ACL web). Si desea cambiar cualquier área, elija el área y seleccione Edit (Editar). Esto le devuelve a la página en el asistente de ACL web. Realice los cambios y, a continuación, haga clic en Next (Siguiente) para pasar las páginas hasta volver a la página Review and create web ACL (Revisar y crear ACL Web).
22. Elija Create web ACL (Crear ACL web). La nueva ACL web aparece en la página Web ACLs .

Edición de una ACL web

Para agregar o eliminar reglas de una ACL web o cambiar los ajustes de configuración, acceda a la ACL web mediante el procedimiento de esta página. Al actualizar una ACL web, AWS WAF proporciona cobertura continua a los recursos que tiene asociados a la ACL web.

Riesgo de tráfico de producción

Antes de implementar cambios en su ACL web para el tráfico de producción, pruébelos y ajústelos en un entorno provisional o de pruebas hasta que se sienta cómodo con el posible impacto en el tráfico. A continuación, pruebe y ajuste las reglas actualizadas en el modo de recuento con el tráfico de producción antes de habilitarlas. Para obtener instrucciones, consulte Probando y ajustando sus AWS WAF protecciones.

Note

El uso de más de 1500 WCU en una ACL web conlleva costos superiores al precio de la ACL web básica. Para obtener más información, consulte AWS WAF unidades de capacidad ACL web (WCU) y Precios de AWS WAF.

Para editar una ACL web

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, seleccione Web ACLs (ACL web).
3. Elegir el nombre de la ACL web que desea editar. La consola le lleva a la descripción de la ACL web.

   > **Note**
   >
   > Las ACL web que se administran mediante AWS Firewall Manager tienen nombres que comienzan `FMManagedWebACLV2-` por. El administrador del Firewall Manager los gestiona en las AWS WAF políticas del Firewall Manager. Estas ACL web pueden contener conjuntos de grupos de reglas designados para ejecutarse en primer y último lugar en la ACL web, a ambos lados de las reglas o grupos de reglas que agregue y administre. No puede cambiar ninguna de estas especificaciones del primer y último grupo de reglas. El primer y el último grupo de reglas tienen nombres que comienzan por `PREFMManaged-` y `POSTFMManaged-`, respectivamente. Para obtener más información sobre estas políticas, consulte AWS WAF políticas.

4. Edite la ACL web según sea necesario. Seleccione las pestañas de las áreas de configuración que le interesen y edite las configuraciones mutables. Para cada configuración que edite, al seleccionar Guardar y volver a la página de descripción de la ACL web, la consola guardará los cambios en la ACL web.

   A continuación, se enumeran las pestañas que contienen los componentes de configuración de la ACL web.

   - Pestaña Reglas
     - Reglas definidas en la ACL web: Puede editar y administrar las reglas que ha definido en la ACL web de forma similar a como lo hizo durante la creación de la ACL web.

       > **Note**
       >
       > No cambie los nombres de ninguna regla que no haya agregado manualmente a su ACL web. Si utiliza otros servicios para administrar las reglas por usted, cambiar sus nombres podría eliminar o reducir su capacidad de proporcionar las protecciones previstas. AWS Shield Advanced y AWS Firewall Manager ambos

crean reglas en su ACL web. Para obtener más información, consulte Grupos de reglas proporcionados por otros servicios.

> **Note**
>
> Si cambia el nombre de una regla y desea que el nombre de la métrica de la regla refleje el cambio, también debe actualizar el nombre de la métrica. AWS WAF no actualiza automáticamente el nombre de la métrica de una regla cuando se cambia el nombre de la regla. Puede cambiar el nombre de la métrica al editar la regla en la consola mediante el editor de reglas de JSON. También puede cambiar ambos nombres a través de las API y en cualquier lista de JSON que utilice para definir su ACL web o grupo de reglas.

Para obtener información sobre la configuración de las reglas y los grupos de reglas, consulte AWS WAF reglas y AWS WAF grupos de reglas.

- Unidades de capacidad de reglas de la ACL web utilizadas: el uso de la capacidad actual de su ACL web. Esto es solo para visualización.
- Acción de ACL web predeterminada para las solicitudes que no coinciden con ninguna regla: para obtener información sobre esta configuración, consulte La acción predeterminada de ACL web.
- Configuraciones de CAPTCHA y desafíos de ACL web: estos tiempos de inmunidad determinan cuánto tiempo permanece válido un token de CAPTCHA o desafío después de su adquisición. Solamente puede modificar esta configuración aquí, después de crear la ACL web. Para obtener más información sobre esta configuración, consulte Caducidad de la marca de tiempo: tiempos de inmunidad AWS WAF simbólica.
- Lista de dominios simbólicos: AWS WAF acepta identificadores para todos los dominios de la lista y para el dominio del recurso asociado. Para obtener más información, consulte AWS WAF Configuración de la lista de dominios del token ACL web.

- Pestaña de AWS recursos asociados
  - Límite de tamaño de inspección de las solicitudes web: se incluye solo para las ACL web que protegen las CloudFront distribuciones. El límite de tamaño para la inspección de la carrocería determina qué parte del componente de la carrocería se envía AWS WAF para

su inspección. Para obtener más información sobre esta configuración, consulte Gestión de los límites de tamaño de la inspección corporal.

- AWS Recursos asociados: la lista de recursos a los que la ACL web está asociada actualmente y que protege. Puede localizar los recursos que se encuentran dentro de la misma región que la ACL web y asociarlos a la ACL web. Para obtener más información, consulte Asociar o desasociar una ACL web a un recurso AWS.

- Pestaña Cuerpos de respuesta personalizados
  - Cuerpos de respuesta personalizados que están disponibles para que los utilicen las reglas de ACL web que tienen la acción establecida en Block. Para obtener más información, consulte Respuestas personalizadas para las acciones Block.
- Pestaña Registro y métricas
  - Registro: registro del tráfico que evalúa la ACL web. Para obtener más información, consulte Registro del tráfico de ACL AWS WAF web.
  - Solicitudes de muestra: información sobre las reglas que coinciden con las solicitudes web. Para obtener información sobre cómo ver las solicitudes muestreadas, consulte Visualizar una muestra de solicitudes web.
  - CloudWatch métricas: métricas de las reglas de su ACL web. Para obtener información sobre CloudWatch las métricas de Amazon, consultaMonitorización con Amazon CloudWatch.

Incoherencias temporales durante las actualizaciones

Al crear o cambiar una ACL web u otros AWS WAF recursos, los cambios tardan un poco en propagarse a todas las áreas donde se almacenan los recursos. El tiempo de propagación puede oscilar entre unos segundos y varios minutos.

A continuación, se proporcionan ejemplos de incoherencias temporales que podría notar durante la propagación de los cambios:

- Después de crear una ACL web, si intenta asociarla a un recurso, es posible que se produzca una excepción que indique que la ACL web no está disponible.
- Después de agregar un grupo de reglas a una ACL web, las nuevas reglas del grupo de reglas pueden estar en vigor en un área en la que se usa la ACL web y no en otra.
- Tras cambiar la configuración de una acción de regla, es posible que vea la acción anterior en algunos lugares y la acción nueva en otros.

- Después de agregar una dirección IP a un conjunto de IP que está en uso dentro de una regla de bloqueo, es posible que la nueva dirección se bloquee en un área, pero que se permita en otra.

Administrar el comportamiento del grupo de reglas en una ACL web

En esta sección se describen las opciones para modificar cómo se utiliza un grupo de reglas en la ACL web. Esta información se aplica a todos los tipos de grupos de reglas. Después de agregar un grupo de reglas a una ACL web, puede sustituir las acciones de reglas individuales del grupo de reglas por Count o por cualquier otra configuración de acción de regla válida. También puede sustituir la acción resultante del grupo de reglas por Count, lo que no afecta a la forma en que se evalúan las reglas dentro del grupo de reglas.

Para obtener información sobre estas opciones, consulte Opciones de anulación de acciones para grupos de reglas.

Invalidar acciones de reglas en un grupo de reglas

Para cada grupo de reglas de una ACL web, puede anular las acciones de la regla contenida para algunas o todas las reglas.

El caso de uso más común es sustituir las acciones de la regla por Count para probar reglas nuevas o actualizadas. Si tienes las métricas habilitadas, recibirás las métricas de cada regla que anules. Para obtener más información acerca las pruebas, consulte Probando y ajustando sus AWS WAF protecciones.

Acciones de anular regla en un grupo de reglas

Puede realizar estos cambios al agregar un grupo de reglas administrado a la ACL web y puede hacerlos en cualquier tipo de grupo de reglas al editar la ACL web. Estas instrucciones son para un grupo de reglas que ya se ha agregado a la ACL web. Consulte información adicional sobre esta opción enLa acción de la regla del grupo de reglas anula.

1. Edite la ACL web.
2. En la pestaña Reglas de la página ACL web, seleccione el grupo de reglas y, a continuación, elija Editar.
3. En la sección Reglas del grupo de reglas, administre la configuración de las acciones según sea necesario.

- Todas las reglas: para establecer una acción de anulación para todas las reglas del grupo de reglas, abra el menú desplegable Anular todas las acciones de reglas y seleccione la acción de anulación. Para eliminar las anulaciones de todas las reglas, seleccione Eliminar todas las anulaciones.
- Regla única: para configurar una acción de anulación para una sola regla, abra el menú desplegable de la regla y seleccione la acción de anulación. Para eliminar una anulación de una regla, abra el menú desplegable de la regla y seleccione Eliminar la anulación.

4. Cuando haya terminado de realizar los cambios, seleccione Guardar regla. La configuración de la acción de regla y de la acción de anulación se muestra en la página del grupo de reglas.

El siguiente ejemplo de lista JSON muestra una instrucción de grupo de reglas dentro de una ACL web que sustituye por Count las acciones de reglas `CategoryVerifiedSearchEngine` y `CategoryVerifiedSocialMedia`. En la JSON, se anulan todas las acciones de reglas proporcionando una entrada de `RuleActionOverrides` para cada regla individual.

```
{
    "Name": "AWS-AWSBotControl-Example",
   "Priority": 5,
   "Statement": {
    "ManagedRuleGroupStatement": {
        "VendorName": "AWS",
        "Name": "AWSManagedRulesBotControlRuleSet",
        "RuleActionOverrides": [
          {
            "ActionToUse": {
              "Count": {}
            },
            "Name": "CategoryVerifiedSearchEngine"
          },
          {
            "ActionToUse": {
              "Count": {}
            },
            "Name": "CategoryVerifiedSocialMedia"
          }
        ],
        "ExcludedRules": []
    },
   "VisibilityConfig": {
```

```
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSBotControl-Example"
    }
}
```

Sustitución del resultado de la evaluación de un grupo de reglas por Count

Puede anular la acción derivada de la evaluación de un grupo de reglas sin alterar la forma en que se configuran o evalúan las reglas del grupo de reglas. Esta opción no se utiliza habitualmente. Si alguna regla del grupo de reglas da como resultado una coincidencia, esta anulación establece la acción resultante del grupo de reglas en Count.

> **Note**
>
> Este es un caso de uso poco común. La mayoría de las anulaciones de acciones se realizan a nivel de regla, dentro del grupo de reglas, como se describe enInvalidar acciones de reglas en un grupo de reglas.

Puede anular la acción resultante del grupo de reglas en la ACL web al agregar o editar el grupo de reglas. En la consola, abra el panel Anular la acción del grupo de reglas (opcional) del grupo de reglas y habilite la anulación. En la JSON, establezca `OverrideAction` en la instrucción del grupo de reglas, tal y como se muestra en la siguiente lista de ejemplo:

```
{
   "Name": "AWS-AWSBotControl-Example",
   "Priority": 5,
   "Statement": {
    "ManagedRuleGroupStatement": {
     "VendorName": "AWS",
     "Name": "AWSManagedRulesBotControlRuleSet"
     }
   },
    "OverrideAction": {
       "Count": {}
    },
   "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSBotControl-Example"
```

```
    }
}
```

Asociar o desasociar una ACL web a un recurso AWS

Puede utilizarlas AWS WAF para crear las siguientes asociaciones entre las ACLS web y sus recursos:

- Asocie una ACL web regional a cualquiera de los recursos regionales que se indican a continuación. Para esta opción, la ACL web debe estar en la misma región que su recurso.
  - API de REST de Amazon API Gateway
  - Equilibrador de carga de aplicación
  - AWS AppSync API GraphQL
  - Grupo de usuarios de Amazon Cognito
  - AWS App Runner servicio
  - AWS Instancia de acceso verificado
- Asocie una ACL web global a una CloudFront distribución de Amazon. La ACL web global tendrá una región con codificación rígida de Este de EE. UU. (Norte de Virginia).

También puede asociar una ACL web a una CloudFront distribución al crear o actualizar la propia distribución. Para obtener más información, consulta AWS WAF Cómo controlar el acceso a tu contenido en la Guía para CloudFront desarrolladores de Amazon.

Restricciones a varias asociaciones

Puede asociar una única ACL web a uno o más AWS recursos, de acuerdo con las siguientes restricciones:

- Puede asociar cada AWS recurso a una sola ACL web. La relación entre la ACL web y AWS los recursos es one-to-many.
- Puede asociar una ACL web a una o más CloudFront distribuciones. No puede asociar una ACL web que haya asociado a una CloudFront distribución con ningún otro tipo de AWS recurso.

Restricciones adicionales

Se aplican las siguientes restricciones adicionales a las asociaciones de ACL web:

- Solamente puede asociar una ACL web a un equilibrador de carga de aplicación que se encuentre en Regiones de AWS. Por ejemplo, solamente puede asociar una ACL web a un equilibrador de carga de aplicación que se encuentre en AWS Outposts.
- No puede asociar un grupo de usuarios de Amazon Cognito a una ACL web que utilice el grupo de reglas gestionado por la prevención de AWS WAF fraudes para la creación de cuentas (ACFP) de Fraud Control `AWSManagedRulesACFPRuleSet` o el grupo de reglas gestionado por la prevención de apropiación de cuentas (ATP) de AWS WAF Fraud Control. `AWSManagedRulesATPRuleSet` Para obtener información sobre la prevención del fraude en la creación de cuentas, consulte AWS WAF Control de fraude: creación de cuentas y prevención del fraude (ACFP). Para obtener información sobre la prevención de apropiación de cuentas, consulte AWS WAF Control de fraudes y prevención de apropiación de cuentas (ATP).

⚠ Riesgo de tráfico de producción

Antes de implementar cambios en su ACL web para el tráfico de producción, pruébelos y ajústelos en un entorno provisional o de prueba hasta que se sienta cómodo con el posible impacto en el tráfico. A continuación, pruebe y ajuste sus reglas en el modo de recuento con el tráfico de producción antes de habilitarlas. Para obtener instrucciones, consulte Probando y ajustando sus AWS WAF protecciones.

Para asociar una ACL web a un recurso AWS

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, seleccione Web ACLs (ACL web).
3. Elija el nombre de la ACL web que desee asociar a un recurso. La consola le lleva a la descripción de la ACL web, donde puede editarla.
4. En la pestaña AWS Recursos asociados, selecciona Agregar AWS recursos.
5. Cuando se le solicite, elija el tipo de recurso, seleccione el botón de opción situado junto al recurso que desea asociar y, a continuación, elija Agregar.

Para desasociar una ACL web de un recurso AWS

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

2. En el panel de navegación, seleccione Web ACLs (ACL web).
3. Elija el nombre de la ACL web que desee desasociar del recurso. La consola le lleva a la descripción de la ACL web, donde puede editarla.
4. En la pestaña AWS Recursos asociados, seleccione el recurso del que desee desasociar esta ACL web.

> **Note**
>
> Debe desasociar un recurso a la vez. No elija varios recursos.

5. Elija Disociar. La consola abrirá un cuadro de diálogo de confirmación. Confirme su elección de desasociar la ACL web del AWS recurso.

Eliminación de una ACL web

Para eliminar una ACL web, primero debe desasociar todos los AWS recursos de la ACL web. Realice el siguiente procedimiento.

Para eliminar una ACL web

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, seleccione Web ACLs (ACL web).
3. Seleccione el nombre de la ACL web que desea eliminar. La consola le lleva a la descripción de la ACL web, donde puede editarla.
4. En la pestaña AWS Recursos asociados, para cada recurso asociado, selecciona el botón de radio situado junto al nombre del recurso y, a continuación, selecciona Desasociar. Esto disocia la ACL web de sus recursos. AWS
5. En el panel de navegación, seleccione Web ACLs (ACL web).
6. Seleccione el botón de opción situado junto a la ACL web que va a eliminar y, a continuación, elija Delete (Eliminar).

AWS WAF grupos de reglas

Un grupo de reglas es un conjunto de reglas reutilizable que puede agregar a una ACL web. Para obtener más información acerca de las ACL web, consulte AWS WAF listas de control de acceso web (ACL web).

Los grupos de reglas se dividen en las categorías principales:

- Grupos de reglas que crea y mantiene.
- Grupos de reglas AWS administradas que los equipos de reglas administradas crean y mantienen para usted.
- Grupos de reglas gestionados que AWS Marketplace los vendedores crean y mantienen para ti.
- Grupos de reglas que son propiedad y están administrados por otros servicios, como AWS Firewall Manager Shield Advanced.

Diferencias entre grupos de reglas y ACL web

Los grupos de reglas y las ACL web contienen reglas. Estas se definen de la misma manera en ambos lugares. Los grupos de reglas difieren de las ACL web de las siguientes maneras:

- Los grupos de reglas no pueden contener instrucciones de referencia de grupos de reglas.
- Puede reutilizar un solo grupo de reglas en varias ACL web. Para ello, agregue una instrucción de referencia de grupo de reglas a cada ACL web. No puede reutilizar una ACL web.
- Los grupos de reglas no tienen acciones predeterminadas. En una ACL web, se establece una acción predeterminada para cada regla o grupo de reglas que se incluya. Cada regla individual dentro de un grupo de reglas o ACL web tiene una acción definida.
- No asocias directamente un grupo de reglas a un AWS recurso. Para proteger recursos mediante un grupo de reglas, utilice el grupo de reglas en una ACL web.
- Las ACL web tienen una capacidad máxima definida por el sistema de 5000 unidades de capacidad de ACL web (WCU). Cada grupo de reglas tiene una configuración de WCU que debe establecerse en la creación. Puede utilizar esta configuración para calcular los requisitos de capacidad adicionales que el uso de un grupo de reglas agregaría a la ACL web. Para obtener más información acerca de las WCU, consulte AWS WAF unidades de capacidad ACL web (WCU).

Para obtener más información acerca de las reglas, consulte AWS WAF reglas.

En esta sección se proporciona orientación para crear y gestionar sus propios grupos de reglas, describe los grupos de reglas gestionados que están disponibles y se proporciona orientación para utilizar los grupos de reglas gestionados.

Temas

Grupos de reglas administrados

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 El precio básico se aplica al uso de cualquier grupo de reglas gestionado. Para obtener información sobre AWS WAF precios, consulte AWS WAF Precios.

- Los grupos de reglas de AWS Managed Rules para el control de AWS WAF bots, AWS WAF la prevención de apropiación de cuentas (ATP) y la prevención del AWS WAF fraude en la creación de cuentas (ACFP) de Fraud Control están disponibles por cargos adicionales, además de los cargos básicos AWS WAF . Para obtener más información sobre precios, consulte precios de AWS WAF.
- Todos los demás grupos de reglas de AWS Managed Rules están disponibles para AWS WAF los clientes sin coste adicional.
- AWS Marketplace Los grupos de reglas gestionados están disponibles mediante suscripción a través de AWS Marketplace. Cada uno de estos grupos de reglas es propiedad del AWS Marketplace vendedor y está gestionado por él. Para obtener información sobre precios y utilizar un grupo de reglas AWS Marketplace gestionado, ponte en contacto con el AWS Marketplace vendedor.

Algunos grupos de reglas gestionados están diseñados para ayudar a proteger tipos específicos de aplicaciones webWordPress, como Joomla o PHP. Otros ofrecen una amplia protección frente a amenazas conocidas o vulnerabilidades de aplicaciones web comunes, que incluyen algunas de las que se enumeran en OWASP Top 10. Si está sujeto a la conformidad normativa de PCI o HIPAA, podría utilizar grupos de reglas administrados para cumplir los requisitos de firewall de las aplicaciones web.

Actualizaciones automáticas

Mantenerse al día del panorama de amenazas en constante cambio puede resultar lento y costoso. Los grupos de reglas gestionadas le permiten ahorrar tiempo a la hora de implementar y utilizar AWS WAF. Muchos AWS AWS Marketplace vendedores actualizan automáticamente los grupos de reglas administrados y proporcionan nuevas versiones de los grupos de reglas cuando surgen nuevas vulnerabilidades y amenazas.

En algunos casos, AWS se le notifican las nuevas vulnerabilidades antes de su divulgación pública, debido a su participación en varias comunidades de divulgación privada. En esos casos, AWS puede actualizar los grupos de reglas de AWS Managed Rules e implementarlos por usted incluso antes de que se conozca ampliamente una nueva amenaza.

Acceso restringido a las reglas en un grupo de reglas administrado

Cada grupo de reglas administrado ofrece una descripción completa de los tipos de ataques y vulnerabilidades para los que se ha diseñado. Para proteger la propiedad intelectual de los proveedores de grupos de reglas, no puede ver todos los detalles de las reglas individuales que hay dentro de un grupo de reglas. Esta restricción también ayuda a impedir que usuarios malintencionados diseñen amenazas que eludan específicamente las reglas publicadas.

Temas

- Grupos de reglas gestionados versionados
- Trabajar con grupos de reglas administrados
- AWS Reglas administradas para AWS WAF
- AWS Marketplace grupos de reglas gestionados

Grupos de reglas gestionados versionados

Muchos proveedores de grupos de reglas administrados utilizan el control de versiones para actualizar las opciones y capacidades de un grupo de reglas. Por lo general, una versión específica de un grupo de reglas administrado es estática. En ocasiones, es posible que un proveedor necesite actualizar algunas o todas las versiones estáticas de un grupo de reglas administrado, por ejemplo, para responder a una amenaza de seguridad emergente.

Cuando utiliza un grupo de reglas gestionado con versiones en su ACL web, puede seleccionar la versión predeterminada y dejar que el proveedor administre la versión estática que utilice, o puede seleccionar una versión estática específica.

¿No encuentra la versión que busca?

Si no ve una versión en la lista de versiones de un grupo de reglas, es probable que la versión esté programada para caducar o que ya haya caducado. Una vez programada la caducidad de una versión, ya AWS WAF no le permite elegirla para el grupo de reglas.

Notificaciones de SNS para grupos de reglas de AWS Managed Rules

Todos los grupos de reglas de reglas AWS administradas proporcionan notificaciones de control de versiones y actualizaciones de SNS, excepto el grupo de reglas de reputación IP. Todos los grupos de reglas de AWS Managed Rules que proporcionan notificaciones utilizan el mismo tema de SNS: Amazon Resource Name (ARN). Para suscribirse a las notificaciones de SNS, consulte. Recepción de notificaciones sobre nuevas versiones y actualizaciones

Temas

- Ciclo de vida de las versiones para los grupos de reglas administrados
- Caducidad de la versión para los grupos de reglas gestionados
- Prácticas recomendadas para gestionar las versiones de los grupos de reglas administrados

Ciclo de vida de las versiones para los grupos de reglas administrados

Los proveedores gestionan las siguientes etapas del ciclo de vida de una versión estática de un grupo de reglas administrado:

- Versión y actualizaciones: un proveedor de grupos de reglas administrados anuncia las versiones estáticas nuevas y futuras de sus grupos de reglas administrados mediante notificaciones a un tema de Amazon Simple Notification Service (Amazon SNS). Los proveedores también pueden utilizar el tema para comunicar otra información importante sobre sus grupos de reglas, como las actualizaciones que se requieren con urgencia.

  Puede suscribirse al tema del grupo de reglas y configurar la forma en que desea recibir las notificaciones. Para más información, consulte Recepción de notificaciones sobre nuevas versiones y actualizaciones.
- Programación de la caducidad: un proveedor de grupos de reglas administrados programa la caducidad de las versiones anteriores de un grupo de reglas. No se puede agregar una versión que esté programada para caducar a las reglas de la ACL web. Una vez programada la caducidad de una versión, AWS WAF realiza un seguimiento de la caducidad con una métrica de cuenta regresiva en Amazon CloudWatch.

- Caducidad de la versión: si tiene una ACL web configurada para usar una versión caducada de un grupo de reglas administrado, durante la evaluación de la ACL web, AWS WAF utilizará la versión predeterminada del grupo de reglas. Además, AWS WAF bloquea cualquier actualización de la ACL web que no elimine el grupo de reglas ni cambie su versión por una que no haya caducado.

Si usa grupos de reglas AWS Marketplace administrados, solicite al proveedor cualquier información adicional sobre los ciclos de vida de las versiones.

Caducidad de la versión para los grupos de reglas gestionados

Si usa una versión específica de un grupo de reglas, asegúrese de no seguir usando una versión después de su fecha de caducidad. Puedes supervisar la caducidad de las versiones mediante las notificaciones de SNS del grupo de reglas y mediante las CloudWatch métricas de Amazon.

Si una versión que está utilizando en una ACL web ha caducado, AWS WAF bloquea cualquier actualización de la ACL web que no incluya el traslado del grupo de reglas a una versión que no haya caducado. Puede actualizar el grupo de reglas a una versión disponible o eliminarlo de su ACL web.

La gestión de la caducidad de un grupo de reglas administrado depende del proveedor del grupo de reglas. En el AWS caso de los grupos de reglas administradas, una versión caducada se cambia automáticamente a la versión predeterminada del grupo de reglas. En el AWS Marketplace caso de los grupos de reglas, pregunte al proveedor cómo gestiona la caducidad.

Cuando el proveedor crea una nueva versión del grupo de reglas, establece la vida útil prevista de la versión. Si bien la versión no está programada para caducar, el valor de la CloudWatch métrica de Amazon se establece en la configuración de vida útil prevista y CloudWatch, en, verás un valor fijo para la métrica. Una vez que el proveedor programa el vencimiento de la métrica, el valor de la métrica disminuye cada día hasta llegar a cero el día de la caducidad. Para obtener información sobre la supervisión de la caducidad, consulteSeguimiento de la caducidad de la versión.

Prácticas recomendadas para gestionar las versiones de los grupos de reglas administrados

Siga esta guía de prácticas recomendadas para gestionar el control de versiones cuando utilice un grupo de reglas administrado con control de versiones.

Cuando usa un grupo de reglas administrado en su ACL web, puede elegir usar una versión estática específica del grupo de reglas o puede optar por usar la versión predeterminada:

- Versión predeterminada: AWS WAF siempre establece la versión predeterminada en la versión estática recomendada actualmente por el proveedor. Cuando el proveedor actualiza la versión estática recomendada, AWS WAF actualiza automáticamente la configuración de la versión predeterminada para el grupo de reglas de su ACL web.

  Cuando utilice la versión predeterminada de un grupo de reglas administrado, siga los pasos a continuación como práctica recomendada:

  - Suscribirse a las notificaciones: suscríbase a las notificaciones de cambios en el grupo de reglas y esté pendiente. La mayoría de los proveedores envían notificaciones avanzadas sobre las nuevas versiones estáticas y los cambios en las versiones predeterminadas. Estas permiten comprobar los efectos de una nueva versión estática antes AWS de cambiar a la versión predeterminada. Para más información, consulte Recepción de notificaciones sobre nuevas versiones y actualizaciones.
  - Revise los efectos de la configuración de la versión estática y realice los ajustes necesarios antes de establecer la versión predeterminada: antes de establecer una nueva versión estática como predeterminada, revise los efectos de la versión estática en la supervisión y la administración de las solicitudes web. Es posible que la nueva versión estática tenga nuevas reglas que revisar. En caso de que necesite modificar la forma en que utiliza el grupo de reglas, busque falsos positivos u otros comportamientos inesperados. Puede establecer reglas de recuento, por ejemplo, para evitar que bloqueen el tráfico mientras decide cómo quiere gestionar el nuevo comportamiento. Para obtener más información, consulte Probando y ajustando sus AWS WAF protecciones.
- Versión estática: si elige usar una versión estática, debe actualizar manualmente la configuración de la versión cuando esté listo para adoptar una nueva versión del grupo de reglas.

  Cuando utilice una versión estática de un grupo de reglas administrado, haga lo siguiente como práctica recomendada:

  - Mantener la versión actualizada: mantenga su grupo de reglas administrado lo más cerca posible de la última versión. Cuando se publique una nueva versión, pruébela, ajuste la configuración según sea necesario e impleméntela de manera oportuna. Para obtener información acerca de las pruebas, consulte Probando y ajustando sus AWS WAF protecciones.
  - Suscribirse a las notificaciones: suscríbase a las notificaciones de cambios en el grupo de reglas para saber cuándo su proveedor lanza nuevas versiones estáticas. La mayoría de los proveedores notifican con antelación los cambios de versión. Además, es posible que su proveedor necesite actualizar la versión estática que está utilizando para cerrar una laguna de seguridad o por otros motivos urgentes. Sabrá lo que sucede si está suscrito a las notificaciones

del proveedor. Para obtener más información, consulte Recepción de notificaciones sobre nuevas versiones y actualizaciones.

- Evita la caducidad de la versión: no permita que una versión estática caduque mientras la usa. La gestión por parte del proveedor de las versiones caducadas puede variar y puede implicar forzar la actualización a una versión disponible u otros cambios que puedan tener consecuencias inesperadas. Realice un seguimiento de la métrica de AWS WAF caducidad y configure una alarma que le dé un número de días suficiente para actualizar correctamente a una versión compatible. Para obtener más información, consulte Seguimiento de la caducidad de la versión.

Trabajar con grupos de reglas administrados

En esta sección se proporciona orientación para acceder a su grupos de reglas administrados y administrarlos.

Cuando agrega un grupo de reglas administrado a su ACL web, puede elegir las mismas opciones de configuración que sus propios grupos de reglas, además de configuraciones adicionales.

A través de la consola, puede acceder a la información de los grupos de reglas administrados durante el proceso de agregar y editar las reglas en sus ACL web. A través de las API y la interfaz de la línea de comandos (CLI), puede solicitar directamente información sobre los grupos de reglas administrados.

Cuando usa un grupo de reglas administrado en su ACL web, puede editar las siguientes configuraciones:

- Versión: solo está disponible si el grupo de reglas presenta control de versiones. Para obtener más información, consulte Grupos de reglas gestionados versionados.
- Acciones de anular regla: puede sustituir las acciones de reglas del grupo de reglas por cualquier acción. Definirlas en Count es útil para probar un grupo de reglas antes de usarlo para administrar las solicitudes web. Para obtener más información, consulte La acción de la regla del grupo de reglas anula.
- Declaración de alcance reducido: puede añadir una declaración de alcance reducido, para filtrar las solicitudes web que no desee evaluar con el grupo de reglas. Para obtener más información, consulte Instrucciones de restricción de acceso.
- Invalidar la acción del grupo de reglas: puede anular la acción que se deriva de la evaluación del grupo de reglas y configurarla solo como Count. Esta opción no se utiliza habitualmente. No

altera la forma en que AWS WAF se evalúan las reglas del grupo de reglas. Para obtener más información, consulte El grupo de reglas devuelve la acción de anulación a Count.

Edición de la configuración del grupo de reglas administrado en su ACL web

- Consola
  - (Opción) Cuando agrega el grupo de reglas administrado a su ACL web, puede elegir Editar para ver y editar la configuración.
  - (Opción) Tras agregar el grupo de reglas administrado a la ACL web, en la página ACL web, elija la ACL web que acaba de crear. Esto le lleva a la página web de edición de ACL web.
    - Elija Rules (Reglas).
    - Seleccione el grupo de reglas y, a continuación, elija Editar para ver y editar la configuración.
- API y CLI: fuera de la consola, puede administrar la configuración la configuración del grupo de reglas administrado al crear y actualizar la ACL web.

Recuperación de la lista de grupos de reglas administrados

Puede recuperar la lista de grupos de reglas administrados que están disponibles para su uso en las ACL web. La lista incluye lo siguiente:

- Todos los grupos de reglas de reglas AWS administradas.
- Los grupos de AWS Marketplace reglas a los que se ha suscrito.

> **Note**
>
> Para obtener información sobre la suscripción a grupos de AWS Marketplace reglas, consulte. AWS Marketplace grupos de reglas gestionados

Al recuperar la lista de grupos de reglas administrados, la lista que obtenga dependerá de la interfaz que utilice:

- Consola: a través de la consola, puede ver todos los grupos de reglas administrados, incluidos los grupos de AWS Marketplace reglas a los que aún no se ha suscrito. Para aquellos a los que aún no se haya suscrito, la interfaz proporciona enlaces que puede seguir para suscribirse.

- API y CLI: fuera de la consola, la solicitud devuelve solo los grupos de reglas que están disponibles para su uso.

Recuperación de la lista de grupos de reglas administrados

- Consola: durante el proceso de creación de una ACL web, en la página Añadir reglas y grupos de reglas, elija Añadir grupos de reglas administrados. En el nivel superior, se enumeran los nombres de los proveedores. Expanda cada descripción de proveedores para ver la lista de grupos de reglas administrados. En el caso de los grupos de reglas con control de versiones, la información que se muestra en este nivel corresponde a la versión predeterminada. Cuando agrega un grupo de reglas administrado a la ACL web, la consola lo añade a una lista según el esquema de nomenclatura `<Vendor Name>-<Managed Rule Group Name>`.
- API:
  - `ListAvailableManagedRuleGroups`
- CLI:
  - `aws wafv2 list-available-managed-rule-groups --scope=<CLOUDFRONT|REGIONAL>`

Recuperar las reglas de un grupo de reglas administrado

Puede recuperar una lista de reglas de un grupo de reglas administrado. Las llamadas a la API y a la CLI devuelven las especificaciones de las reglas a las que puede hacer referencia en el modelo JSON o a través de él AWS CloudFormation.

Para recuperar la lista de reglas de un grupo de reglas administrado

- Consola
  - (Opción) Cuando agrega el grupo de reglas administradas a su ACL web, puede elegir Editar para ver las reglas.
  - (Opción) Tras agregar el grupo de reglas administrado a la ACL web, en la página ACL web, elija la ACL web que acaba de crear. Esto le lleva a la página web de edición de ACL web.
    - Elija Rules (Reglas).
    - Seleccione el grupo de reglas del que desee ver una lista de reglas y, a continuación, elija Editar. AWS WAF muestra la lista de reglas del grupo de reglas.
- API: `DescribeManagedRuleGroup`

- CLI: `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Recuperación de las versiones disponibles de un grupo de reglas administrado

Las versiones disponibles de un grupo de reglas administrado son versiones cuya caducidad aún no está programada. Las lista indica qué versión es la predeterminada actual para el grupo de reglas.

Recuperación de una lista de las versiones disponibles de un grupo de reglas administrado

- Consola
  - (Opcional) Cuando añada el grupo de reglas administrado a su ACL web, elija Editar para ver la información del grupo de reglas. Amplíe el menú desplegable Versión para ver la lista de versiones disponibles.
  - (Opción) Tras agregar el grupo de reglas gestionado a la ACL web, seleccione Editar en la ACL web y, a continuación, seleccione y edite la regla del grupo de reglas para ver el ARN del tema de Amazon SNS del grupo de reglas. Amplíe el menú desplegable Versión para ver la lista de versiones disponibles.
- API:
  - `ListAvailableManagedRuleGroupVersions`
- CLI:
  - `aws wafv2 list-available-managed-rule-group-versions --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Adición de un grupo de reglas administrado a una ACL web a través de la consola

Esta guía se aplica a todos los grupos de reglas AWS administradas y a los grupos de AWS Marketplace reglas a los que está suscrito.

⚠ Riesgo de tráfico de producción

Antes de implementar cambios en su ACL web para el tráfico de producción, pruébelos y ajústelos en un entorno provisional o de pruebas hasta que se sienta cómodo con el posible impacto en el tráfico. A continuación, pruebe y ajuste las reglas actualizadas en el modo

de recuento con el tráfico de producción antes de habilitarlas. Para obtener instrucciones, consulte Probando y ajustando sus AWS WAF protecciones.

> **Note**
>
> El uso de más de 1500 WCU en una ACL web conlleva costos superiores al precio de la ACL web básica. Para obtener más información, consulte AWS WAF unidades de capacidad ACL web (WCU) y Precios de AWS WAF.

Cómo añadir un grupo de reglas administrado a una ACL web a través de la consola

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, seleccione Web ACL.
3. En la página ACL web, en la lista de ACL web, seleccione aquella a la que desee agregar el grupo de reglas. Esto le lleva a la página web de edición de la ACL web individual.
4. En la página de configuración de ACL web, elija la pestaña Reglas.
5. En el panel Reglas, seleccione Agregar reglas y, a continuación, elija Agregar grupos de reglas administradas.
6. En la página Agregar grupos de reglas administrados, amplíe la selección del proveedor de grupos de reglas para ver la lista de grupos de reglas disponibles.
7. Para cada grupo de reglas que desee agregar, elija Agregar a ACL web. Si desea cambiar la configuración de la ACL web para el grupo de reglas, elija Editar, realice los cambios y, a continuación, seleccione Guardar regla. Para obtener información sobre las opciones, consulte la guía de control de versiones en Grupos de reglas gestionados versionados y la guía para usar un grupo de reglas administrado en una ACL web en Instrucción de grupo de reglas administrado.
8. En la parte inferior de la página Agregar grupos de reglas administrados, elija Agregar reglas.
9. En la página Establecer la prioridad de las reglas, ajuste el orden en que se ejecutarán las reglas según sea necesario y, a continuación, seleccione Guardar. Para obtener más información, consulte Procesamiento del orden de las reglas y los grupos de reglas en una ACL web.

En la página de su ACL web, los grupos de reglas administrados que ha agregado aparecen en la pestaña Reglas.

Pruebe y ajuste cualquier cambio en sus AWS WAF protecciones antes de utilizarlas para el tráfico de producción. Para obtener más información, consulte Probando y ajustando sus AWS WAF protecciones.

Incoherencias temporales durante las actualizaciones

Al crear o cambiar una ACL web u otros AWS WAF recursos, los cambios tardan un poco en propagarse a todas las áreas donde se almacenan los recursos. El tiempo de propagación puede oscilar entre unos segundos y varios minutos.

A continuación, se proporcionan ejemplos de incoherencias temporales que podría notar durante la propagación de los cambios:

- Después de crear una ACL web, si intenta asociarla a un recurso, es posible que se produzca una excepción que indique que la ACL web no está disponible.
- Después de agregar un grupo de reglas a una ACL web, las nuevas reglas del grupo de reglas pueden estar en vigor en un área en la que se usa la ACL web y no en otra.
- Tras cambiar la configuración de una acción de regla, es posible que vea la acción anterior en algunos lugares y la acción nueva en otros.
- Después de agregar una dirección IP a un conjunto de IP que está en uso dentro de una regla de bloqueo, es posible que la nueva dirección se bloquee en un área, pero que se permita en otra.

Recepción de notificaciones sobre nuevas versiones y actualizaciones de un grupo de reglas administrado

Un proveedor de grupos de reglas gestionados utiliza las notificaciones de SNS para anunciar los cambios en los grupos de reglas, como las próximas nuevas versiones y las actualizaciones de seguridad urgentes.

Cómo suscribirse a las notificaciones de SNS

Para suscribirse a las notificaciones de un grupo de reglas, cree una suscripción de Amazon SNS para el ARN del tema de Amazon SNS del grupo de reglas en la región Este de EE. UU. (Norte de Virginia) us-east-1.

Para obtener información sobre cómo suscribirse, consulte la Guía para desarrolladores de Amazon Simple Notification Service.

> **Note**
>
> Cree su suscripción para el tema SNS únicamente en la región us-east-1.

Todos los grupos de reglas de AWS Managed Rules versionados utilizan el mismo tema de SNS: Amazon Resource Name (ARN). Para obtener más información sobre las notificaciones de los grupos de reglas de AWS Managed Rules, consulte. Notificaciones de despliegue

Dónde encontrar el ARN del tema de Amazon SNS para un grupo de reglas administrado

AWS Los grupos de reglas de reglas administradas utilizan un único ARN de tema de SNS, por lo que puede recuperar el ARN del tema de uno de los grupos de reglas y suscribirse a él para recibir notificaciones de todos los grupos de reglas de reglas de reglas administradas que AWS proporcionan notificaciones de SNS.

- Consola
  - (Opcional) Cuando añada el grupo de reglas administrado a su ACL web, elija Editar para ver la información del grupo de reglas, que incluye el ARN del tema de Amazon SNS del grupo de reglas.
  - (Opción) Tras agregar el grupo de reglas administrado a la ACL web, seleccione Editar en la ACL web y, a continuación, seleccione y edite la regla del grupo de reglas para ver el ARN del tema de Amazon SNS del grupo de reglas.
- API: `DescribeManagedRuleGroup`
- CLI: `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Para obtener información general sobre los formatos de notificación de Amazon SNS y cómo filtrar las notificaciones que recibe, consulte Análisis de formatos de mensajes y las Políticas de filtro de suscripciones de Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

Seguimiento de la caducidad de las versiones de un grupo de reglas

Si usa una versión específica de un grupo de reglas, asegúrese de no seguir usando una versión después de su fecha de caducidad.

> **Tip**
>
> Suscríbase a las notificaciones de Amazon SNS para los grupos de reglas gestionados y manténgase al día con las versiones de los grupos de reglas gestionados. Se beneficiará de la mayor up-to-date protección del grupo de reglas y se adelantará a la fecha de caducidad. Para obtener más información, consulte Recepción de notificaciones sobre nuevas versiones y actualizaciones.

Para supervisar la programación de caducidad de un grupo de reglas gestionado a través de Amazon CloudWatch

1. En CloudWatch, localice las métricas de caducidad de su grupo AWS WAF de reglas gestionado. Las métricas tienen los siguientes nombres y dimensiones:
   - Nombre de métrica: DaysToExpiry
   - Dimensiones de métricas: Region, ManagedRuleGroup, Vendor y Version

   Si tiene un grupo de reglas administrado en su ACL web que evalúa el tráfico, obtendrá una métrica para ello. La métrica no está disponible para los grupos de reglas que no utilices.
2. Configure una alarma en las métricas que le interesen para que reciba una notificación a tiempo para cambiar a una versión más reciente del grupo de reglas.

Para obtener información sobre el uso de CloudWatch las métricas de Amazon y la configuración de alarmas, consulta la Guía del CloudWatch usuario de Amazon.

Ejemplos de configuraciones de grupos de reglas administrados en JSON y YAML

Las llamadas a la API y a la CLI devuelven una lista de todas las reglas del grupo de reglas administrado a las que puede hacer referencia en el modelo JSON o a través de él AWS CloudFormation.

JSON

Puede hacer referencia a grupos de reglas administrados y modificarlos en una instrucción de regla mediante JSON. En la siguiente lista se muestra el grupo de reglas AWS administradas`AWSManagedRulesCommonRuleSet`, en formato JSON. La especificación de RuleActionOverrides muestra una regla cuya acción se ha sustituido por Count.

```
{
    "Name": "AWS-AWSManagedRulesCommonRuleSet",
    "Priority": 0,
    "Statement": {
      "ManagedRuleGroupStatement": {
        "VendorName": "AWS",
        "Name": "AWSManagedRulesCommonRuleSet",
        "RuleActionOverrides": [

          {

            "ActionToUse": {

              "Count": {}

            },

            "Name": "NoUserAgent_HEADER"

          }

        ],
        "ExcludedRules": []
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesCommonRuleSet"
    }
}
```

YAML

Puede hacer referencia a grupos de reglas administrados y modificarlos en una instrucción de regla mediante la plantilla de YAML de AWS CloudFormation . En la siguiente lista se muestra el grupo de reglas AWS administradas`AWSManagedRulesCommonRuleSet`, en la AWS CloudFormation plantilla. La especificación de RuleActionOverrides muestra una regla cuya acción se ha sustituido por Count.

```
Name: AWS-AWSManagedRulesCommonRuleSet
Priority: 0
Statement:
  ManagedRuleGroupStatement:
    VendorName: AWS
    Name: AWSManagedRulesCommonRuleSet
    RuleActionOverrides:
    - ActionToUse:
        Count: {}
      Name: NoUserAgent_HEADER
    ExcludedRules: []
OverrideAction:
  None: {}
VisibilityConfig:
  SampledRequestsEnabled: true
  CloudWatchMetricsEnabled: true
  MetricName: AWS-AWSManagedRulesCommonRuleSet
```

AWS Reglas administradas para AWS WAF

AWS Managed Rules for AWS WAF es un servicio gestionado que proporciona protección contra las vulnerabilidades comunes de las aplicaciones u otro tipo de tráfico no deseado. Tiene la opción de seleccionar uno o más grupos de reglas de las reglas AWS administradas para cada ACL web, hasta el límite máximo de la unidad de capacidad (WCU) de la ACL web.

Mitigación de los falsos positivos y comprobación de los cambios en los grupos de reglas

Antes de usar cualquier grupo de reglas administrado en producción, pruébelo en un entorno que no sea de producción de acuerdo con las instrucciones de Probando y ajustando sus AWS WAF protecciones. Siga las instrucciones de prueba y ajuste cuando agregue un grupo de reglas a su ACL web, para probar una nueva versión de un grupo de reglas y siempre que un grupo de reglas no gestione su tráfico web como lo necesita.

Responsabilidades de seguridad compartidas

AWS Las reglas administradas están diseñadas para protegerlo de las amenazas web más comunes. Cuando se utilizan de acuerdo con la documentación, los grupos de reglas de reglas AWS administradas añaden otro nivel de seguridad a sus aplicaciones. Sin embargo, los grupos de reglas de reglas AWS administradas no pretenden sustituir sus responsabilidades de seguridad, que vienen determinadas por los AWS recursos que seleccione. Consulte el modelo de responsabilidad compartida para asegurarse de que sus recursos AWS estén debidamente protegidos.

AWS Lista de grupos de reglas de Managed Rules

La información que publicamos sobre las reglas de los grupos de reglas de reglas AWS administradas tiene por objeto proporcionarle información suficiente para utilizarlas, pero no proporciona información que los delincuentes puedan utilizar para eludirlas. Si necesita más información de la que se encuentra en esta documentación, póngase en contacto con el centro de AWS Support.

En esta sección se describen las versiones más recientes de los grupos de reglas de reglas AWS administradas. Los verá en la consola al agregar un grupo de reglas administrado a la ACL web. A través de la API, puede recuperar esta lista junto con los grupos de reglas AWS Marketplace administrados a los que está suscrito llamando`ListAvailableManagedRuleGroups`.

> **Note**
>
> Para obtener información sobre cómo recuperar las versiones de un grupo de reglas de reglas AWS administradas, consulte. Recuperación de las versiones disponibles de un grupo de reglas administrado

Todos los grupos de reglas de reglas AWS administradas admiten el etiquetado, y las listas de reglas de esta sección incluyen las especificaciones de las etiquetas. Puede recuperar las etiquetas de un grupo de reglas administrado a través de la API llamando al `DescribeManagedRuleGroup`. Las etiquetas aparecen en la propiedad AvailableLabels de la respuesta. Para obtener más información acerca de las etiquetas, consulte AWS WAF etiquetas en las solicitudes web.

Pruebe y ajuste cualquier cambio en sus AWS WAF protecciones antes de utilizarlas para el tráfico de producción. Para obtener más información, consulte Probando y ajustando sus AWS WAF protecciones.

AWS Reglas administradas: grupos de reglas

- Grupos de reglas de base de referencia
  - Grupo de reglas administrado del conjunto de reglas básicas (CRS)
  - Grupo de reglas administrado de protección de la administración
  - Grupo de reglas administrado de entradas incorrectas conocidas
- Grupos de reglas específicos de casos de uso
  - Grupo de reglas administrado de la base de datos SQL

Grupos de reglas de base de referencia

Los grupos de reglas administrados de base de referencia proporcionan protección general contra una amplia variedad de amenazas comunes. Elija uno o varios de estos grupos de reglas para establecer la protección de base de referencia para los recursos.

> **Note**
>
> La información que publicamos sobre las reglas de los grupos de reglas AWS administradas tiene por objeto proporcionarle suficiente información para utilizarlas, pero no proporciona información que los delincuentes puedan utilizar para eludir las reglas. Si necesita más información de la que se encuentra en esta documentación, póngase en contacto con el centro de AWS Support.

Grupo de reglas administrado del conjunto de reglas básicas (CRS)

VendorName:`AWS`, Nombre:`AWSManagedRulesCommonRuleSet`, WCU: 700

Este grupo de reglas del conjunto de reglas básicas (CRS) contiene reglas que son generalmente aplicables a las aplicaciones web. Este brinda protección contra la explotación de una amplia gama de vulnerabilidades, incluyendo algunas de las vulnerabilidades de alto riesgo y más comunes descritas en publicaciones de OWASP tales como OWASP Top 10. Considere la posibilidad de utilizar este grupo de reglas para cualquier caso de AWS WAF uso.

Este grupo de reglas administrado agrega etiquetas a las solicitudes web que evalúa, que están disponibles para las reglas que se ejecutan después de este grupo de reglas en su ACL web. AWS WAF también registra las etiquetas según las CloudWatch métricas de Amazon. Para obtener información general sobre las etiquetas y las métricas de etiquetas, consulte Etiquetas en las solicitudes web y Etiquetar métricas y dimensiones.

> **Note**
>
> En esta tabla, se describe la versión estática más reciente de este grupo de reglas. Para otras versiones, usa el comando API DescribeManagedRuleGroup.

Nombre de la regla	Descripción y etiqueta
`NoUserAgent_HEADER`	Inspecciona las solicitudes a las que les falta el encabezado HTTP `User-Agent` . Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:NoUserAgent_Header`
`UserAgent_BadBots_HEADER`	Comprueba si hay valores de encabezado `User-Agent` comunes que indiquen que la solicitud es un badbot. Los patrones de ejemplo incluyen `nessus` y `nmap`. Para obtener información sobre la administración de bots, consulte también AWS WAF Grupo de reglas de control de bots. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:BadBots_Header`
`SizeRestrictions_QUERYSTRING`	Inspecciona las cadenas de consulta de URI que superen los 2048 bytes. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:SizeRestrictions_QueryString`
`SizeRestrictions_Cookie_HEADER`	Comprueba si los encabezados de las cookies tienen más de 10 240 bytes. Acción de la regla: Block

Nombre de la regla	Descripción y etiqueta
	Etiqueta: `awswaf:managed:aws:core-rule-set:SizeRestrictions_Cookie_Header`
`SizeRestrictions_BODY`	Inspecciona los cuerpos de las solicitudes que pesen más de 8 KB (8192 bytes). Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:SizeRestrictions_Body`
`SizeRestrictions_URIPATH`	Inspeccione las rutas de URI que superen los 1024 bytes. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:SizeRestrictions_URIPath`

Nombre de la regla	Descripción y etiqueta
`EC2MetaDataSSRF_BODY`	Inspecciona los intentos de sustraer metadatos de Amazon EC2 del cuerpo de la solicitud. **Warning** Esta regla solo inspecciona el cuerpo de la solicitud hasta el límite de tamaño del cuerpo para la ACL web y el tipo de recurso. Para Application Load Balancer y AWS AppSync, el límite se ha fijado en 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner y Verified Access, el límite predeterminado es de 16 KB y puede aumentarlo hasta 64 KB en su configuración de ACL web. Esta regla utiliza la opción `Continue` para gestionar contenido sobredimensionado. Para obtener más información, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Body`

Nombre de la regla	Descripción y etiqueta
`EC2MetaDataSSRF_COOKIE`	Inspecciona los intentos de sustraer metadatos de Amazon EC2 de la cookie de la solicitud. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Cookie`
`EC2MetaDataSSRF_URIPATH`	Inspecciona los intentos de sustraer metadatos de Amazon EC2 de la ruta del URI de la solicitud. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_URIPath`
`EC2MetaDataSSRF_QUERYARGUMENTS`	Inspecciona los intentos de sustraer metadatos de a de los argumentos de consulta de la solicitud. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_QueryArguments`

Nombre de la regla	Descripción y etiqueta
`GenericLFI_QUERYARGUMENTS`	Inspecciona la presencia de vulnerabilidades Local File Inclusion (LFI, Inclusión Local de Archivos) en los argumentos de la consulta. Los ejemplos incluyen los intentos de recorrido de ruta utilizando técnicas como `../../`. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:GenericLFI_QueryArguments`
`GenericLFI_URIPATH`	Inspecciona la presencia de vulnerabilidades Local File Inclusion (LFI, Inclusión Local de Archivos) en la ruta del URI. Los ejemplos incluyen los intentos de recorrido de ruta utilizando técnicas como `../../`. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:GenericLFI_URIPath`

Nombre de la regla	Descripción y etiqueta
`GenericLFI_BODY`	Inspecciona la presencia de vulnerabilidades Local File Inclusion (LFI, Inclusión Local de Archivos) en el cuerpo de la solicitud. Los ejemplos incluyen los intentos de recorrido de ruta utilizando técnicas como `../../`. **Warning** Esta regla solo inspecciona el cuerpo de la solicitud hasta el límite de tamaño del cuerpo para la ACL web y el tipo de recurso. Para Application Load Balancer y AWS AppSync, el límite se ha fijado en 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner y Verified Access, el límite predeterminado es de 16 KB y puede aumentarlo hasta 64 KB en su configuración de ACL web. Esta regla utiliza la opción `Continue` para gestionar contenido sobredimensionado. Para obtener más información, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:GenericLFI_Body`

Nombre de la regla	Descripción y etiqueta
`RestrictedExtensions_URIPATH`	Comprueba si hay solicitudes cuyas rutas de URI contengan extensiones de archivos del sistema que no sean seguras de leer o ejecutar. Los patrones de ejemplo incluyen extensiones como `.log` y `.ini`. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:RestrictedExtensions_URIPath`
`RestrictedExtensions_QUERYARGUMENTS`	Inspecciona las solicitudes cuyos argumentos de consulta contienen extensiones de archivo cuya lectura es insegura. Los patrones de ejemplo incluyen extensiones como `.log` y `.ini`. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:RestrictedExtensions_QueryArguments`

Nombre de la regla	Descripción y etiqueta
`GenericRFI_QUERYARGUMENTS`	Inspecciona los valores de todos los parámetros de consulta para detectar intentos de aprovechar la RFI (Inclusión Remota de Archivos) en aplicaciones web mediante la incrustación de direcciones URL que contienen direcciones IPv4. Los ejemplos incluyen patrones como `http://`, `https://`, `ftp://`, `ftps://` y `file://`, con un encabezado de host IPv4 en el intento de explotación. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:GenericRFI_QueryArguments`

Nombre de la regla	Descripción y etiqueta
`GenericRFI_BODY`	Inspecciona el cuerpo de las solicitudes para detectar intentos de aprovechar la RFI (Inclusión Remota de Archivos) en aplicaciones web mediante la incrustación de direcciones URL que contienen direcciones IPv4. Los ejemplos incluyen patrones como `http://`, `https://`, `ftp://`, `ftps://` y `file://`, con un encabezado de host IPv4 en el intento de explotación. **Warning** Esta regla solo inspecciona el cuerpo de la solicitud hasta el límite de tamaño del cuerpo para la ACL web y el tipo de recurso. Para Application Load Balancer y AWS AppSync, el límite se ha fijado en 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner y Verified Access, el límite predeterminado es de 16 KB y puede aumentarlo hasta 64 KB en su configuración de ACL web. Esta regla utiliza la opción `Continue` para gestionar contenido sobredimensionado. Para obtener más información, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block

Nombre de la regla	Descripción y etiqueta
	Etiqueta: `awswaf:managed:aws:core-rule-set:GenericRFI_Body`
`GenericRFI_URIPATH`	Inspecciona la ruta de URI para detectar intentos de aprovechar la RFI (Inclusión Remota de Archivos) en aplicaciones web mediante la incrustación de direcciones URL que contienen direcciones IPv4. Los ejemplos incluyen patrones como `http://`, `https://`, `ftp://`, `ftps://` y `file://`, con un encabezado de host IPv4 en el intento de explotación. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:GenericRFI_URIPath`

Nombre de la regla	Descripción y etiqueta
`CrossSiteScripting_COOKIE`	Inspecciona los valores de los encabezados de las cookies para detectar patrones comunes de secuencias de comandos entre sitios (XSS) mediante la función integrada. AWS WAF Instrucción de regla de ataques de scripting entre sitios Los patrones de ejemplo incluyen scripts como `<script>alert("hello")</script>` . **Note** Los detalles de coincidencia de reglas de los AWS WAF registros no se rellenan en la versión 2.0 de este grupo de reglas. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_Cookie`

Nombre de la regla	Descripción y etiqueta
`CrossSiteScripting_QUERYARGUMENTS`	Inspecciona los valores de los argumentos de consulta para detectar patrones comunes de secuencias de comandos entre sitios (XSS) mediante la función integrada. AWS WAF Instrucción de regla de ataques de scripting entre sitios Los patrones de ejemplo incluyen scripts como `<script>alert("hello")</script>` . **Note** Los detalles de coincidencia de reglas de los AWS WAF registros no se rellenan en la versión 2.0 de este grupo de reglas. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_QueryArguments`

Nombre de la regla	Descripción y etiqueta
`CrossSiteScripting_BODY`	Inspecciona el cuerpo de la solicitud para detectar patrones comunes de secuencias de comandos entre sitios (XSS) mediante la función integrada. AWS WAF Instrucción de regla de ataques de scripting entre sitios Los patrones de ejemplo incluyen scripts como `<script>alert("hello")</script>` . **Note** Los detalles de coincidencia de reglas de los AWS WAF registros no se rellenan en la versión 2.0 de este grupo de reglas. **Warning** Esta regla solo inspecciona el cuerpo de la solicitud hasta el límite de tamaño del cuerpo para la ACL web y el tipo de recurso. Para Application Load Balancer y AWS AppSync, el límite se ha fijado en 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner y Verified Access, el límite predeterminado es de 16 KB y puede aumentarlo hasta 64 KB en su configuración de ACL web. Esta regla utiliza la opción `Continue` para gestionar contenido sobredimensionado. Para obtener más información, consulte Manejo de componentes

Nombre de la regla	Descripción y etiqueta
	de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_Body`
`CrossSiteScripting_URIPATH`	Inspecciona el valor de la ruta del URI en busca de patrones comunes de secuencias de comandos entre sitios (XSS) mediante la función integrada. AWS WAF Instrucción de regla de ataques de scripting entre sitios Los patrones de ejemplo incluyen scripts como `<script>alert("hello")</script>` . **Note** Los detalles de coincidencia de reglas de los AWS WAF registros no se rellenan en la versión 2.0 de este grupo de reglas. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_URIPath`

Grupo de reglas administrado de protección de la administración

VendorName:`AWS`, Nombre:`AWSManagedRulesAdminProtectionRuleSet`, WCU: 100

Este grupo contiene reglas que permiten bloquear 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.

Este grupo de reglas administrado agrega etiquetas a las solicitudes web que evalúa, que están disponibles para las reglas que se ejecutan después de este grupo de reglas en su ACL web. AWS WAF también registra las etiquetas según las CloudWatch métricas de Amazon. Para obtener información general sobre las etiquetas y las métricas de etiquetas, consulte Etiquetas en las solicitudes web y Etiquetar métricas y dimensiones.

> **Note**
>
> En esta tabla, se describe la versión estática más reciente de este grupo de reglas. Para otras versiones, usa el comando API DescribeManagedRuleGroup.

Nombre de la regla	Descripción y etiqueta
`AdminProtection_URIPATH`	Inspecciona las rutas del URI que generalmente están reservadas para la administración de un servidor web o una aplicación. Entre los patrones de ejemplo se incluye `sqlmanager` . Acción de la regla: Block Etiqueta: `awswaf:managed:aws:admin-protection:AdminProtection_URIPath`

Grupo de reglas administrado de entradas incorrectas conocidas

VendorName:`AWS`, Nombre:`AWSManagedRulesKnownBadInputsRuleSet`, WCU: 200

Este grupo contiene reglas para bloquear los patrones de solicitud que se conocen por no ser válidos y que están asociados a la explotación o el descubrimiento de vulnerabilidades. Esto puede ayudar a reducir el riesgo de que un actor malintencionado descubra una aplicación vulnerable.

Este grupo de reglas administrado agrega etiquetas a las solicitudes web que evalúa, que están disponibles para las reglas que se ejecutan después de este grupo de reglas en su ACL web. AWS WAF también registra las etiquetas según las CloudWatch métricas de Amazon. Para obtener información general sobre las etiquetas y las métricas de etiquetas, consulte Etiquetas en las solicitudes web y Etiquetar métricas y dimensiones.

> **Note**
>
> En esta tabla, se describe la versión estática más reciente de este grupo de reglas. Para otras versiones, usa el comando API DescribeManagedRuleGroup.

Nombre de la regla	Descripción y etiqueta
`JavaDeserializationRCE_HEADER`	Inspecciona las claves y los valores de los encabezados de las solicitudes HTTP para detectar patrones que indiquen intentos de ejecución remota de comandos (RCE) de deserialización en Java, como las vulnerabilidades RCE de Spring Core y Cloud Function (CVE-202222963, CVE-202222965). Entre los patrones de ejemplo se incluye `(java.lang.Runtime).getRuntime().exec("whoami")` . **Warning** Esta regla solo inspecciona los primeros 8 KB de encabezados de solicitudes o los primeros 200 encabezados, el límite que se alcance primero, y utiliza la opción `Continue` para gestionar contenido de gran

Nombre de la regla	Descripción y etiqueta
	tamaño. Para obtener más informaci ón, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:known-bad-inputs:JavaDeserializatio nRCE_Header`

Nombre de la regla	Descripción y etiqueta
`JavaDeserializationRCE_BODY`	Inspecciona los cuerpos de la solicitud para detectar patrones que indiquen intentos de ejecución remota de comandos (RCE) de deserialización en Java, como las vulnerabilidades de RCE de Spring Core y Cloud Function (CVE-202222963, CVE-202222965). Entre los patrones de ejemplo se incluye `(java.lang.Runtime).getRuntime().exec("whoami")` . **Warning** Esta regla solo inspecciona el cuerpo de la solicitud hasta el límite de tamaño del cuerpo para la ACL web y el tipo de recurso. Para Application Load Balancer y AWS AppSync, el límite se ha fijado en 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner y Verified Access, el límite predeterminado es de 16 KB y puede aumentarlo hasta 64 KB en su configuración de ACL web. Esta regla utiliza la opción `Continue` para gestionar contenido sobredimensionado. Para obtener más información, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block

Nombre de la regla	Descripción y etiqueta
	Etiqueta: `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Body`
`JavaDeserializationRCE_URIPATH`	Inspecciona el URI de la solicitud para detectar patrones que indiquen intentos de ejecución remota de comandos (RCE) de deserialización en Java, como las vulnerabilidades de RCE de Spring Core y Cloud Function (CVE-2022 22963, CVE-202222965). Entre los patrones de ejemplo se incluye `(java.lang.Runtime).getRuntime().exec("whoami")` . Acción de la regla: Block Etiqueta: `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_URIPath`
`JavaDeserializationRCE_QUERYSTRING`	Inspecciona la cadena de la solicitud para detectar patrones que indiquen intentos de ejecución remota de comandos (RCE) de deserialización en Java, como las vulnerabilidades de RCE de Spring Core y Cloud Function (CVE-202222963, CVE-202222965). Entre los patrones de ejemplo se incluye `(java.lang.Runtime).getRuntime().exec("whoami")` . Acción de la regla: Block Etiqueta: `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_QueryString`

Nombre de la regla	Descripción y etiqueta
`Host_localhost_HEADER`	Inspecciona el encabezado del host en la solicitud de patrones que indican localhost . Entre los patrones de ejemplo se incluye `localhost` . Acción de la regla: Block Etiqueta: `awswaf:managed:aws:known-bad-inputs:Host_Localhost_Header`
`PROPFIND_METHOD`	Inspecciona el método HTTP en la solicitud de `PROPFIND`, que es un método similar a `HEAD`, pero con la intención adicional de sustraer objetos XML. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:known-bad-inputs:Propfind_Method`
`ExploitablePaths_URIPATH`	Inspecciona la ruta del URI en busca de intentos de acceder a rutas de aplicaciones web vulnerables. Los patrones de ejemplo incluyen rutas como `web-inf`. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:known-bad-inputs:ExploitablePaths_URIPath`

Nombre de la regla	Descripción y etiqueta
`Log4JRCE_HEADER`	Inspecciona las claves y los valores de los encabezados de las solicitudes para detectar la presencia de la vulnerabilidad Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) y protege contra los intentos de ejecución remota de código (RCE). Entre los patrones de ejemplo se incluye `${jndi:ldap://example.com/}` . **Warning** Esta regla solo inspecciona los primeros 8 KB de encabezados de solicitudes o los primeros 200 encabezados, el límite que se alcance primero, y utiliza la opción `Continue` para gestionar contenido de gran tamaño. Para obtener más información, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_Header`

Nombre de la regla	Descripción y etiqueta
`Log4JRCE_QUERYSTRING`	Inspecciona la cadena de consulta para detectar la presencia de la vulnerabilidad Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) y la protege contra los intentos de ejecución remota de códigos (RCE). Entre los patrones de ejemplo se incluye `${jndi:ldap://example.com/}` . Acción de la regla: Block Etiqueta: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_QueryString`

Nombre de la regla	Descripción y etiqueta
`Log4JRCE_BODY`	Inspecciona el cuerpo para detectar la presencia de la vulnerabilidad Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) y la protege contra los intentos de ejecución remota de códigos (RCE). Entre los patrones de ejemplo se incluye `${jndi:ldap://example.com/}` . **Warning** Esta regla solo inspecciona el cuerpo de la solicitud hasta el límite de tamaño del cuerpo para la ACL web y el tipo de recurso. Para Application Load Balancer y AWS AppSync, el límite se ha fijado en 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner y Verified Access, el límite predeterminado es de 16 KB y puede aumentarlo hasta 64 KB en su configuración de ACL web. Esta regla utiliza la opción `Continue` para gestionar contenido sobredimensionado. Para obtener más información, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_Body`

Nombre de la regla	Descripción y etiqueta
`Log4JRCE_URIPATH`	Inspecciona la ruta del URI cuerpo para detectar la presencia de la vulnerabilidad Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) y la protege contra los intentos de ejecución remota de códigos (RCE). Entre los patrones de ejemplo se incluye `${jndi:ldap://example.com/}` . Acción de la regla: Block Etiqueta: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_URIPath`

Grupos de reglas específicos de casos de uso

Los grupos de reglas para casos de uso específicos proporcionan una protección incremental para muchos casos de uso diferentes. AWS WAF Elija los grupos de reglas que correspondan a la aplicación.

> **Note**
>
> La información que publicamos sobre las reglas de los grupos de reglas AWS administradas tiene por objeto proporcionarle suficiente información para utilizarlas, pero no proporciona información que los delincuentes puedan utilizar para eludirlas. Si necesita más información de la que se encuentra en esta documentación, póngase en contacto con el centro de AWS Support.

Grupo de reglas administrado de la base de datos SQL

VendorName:`AWS`, Nombre:`AWSManagedRulesSQLiRuleSet`, WCU: 200

Este grupo contiene reglas para bloquear los patrones de solicitud asociados a la explotación de bases de datos SQL, como los ataques de inyección de código SQL. Este puede ayudar a evitar la

inyección remota de consultas no autorizadas. Valore el uso de este grupo de reglas si la aplicación interactúa con una base de datos SQL.

Este grupo de reglas administrado agrega etiquetas a las solicitudes web que evalúa, que están disponibles para las reglas que se ejecutan después de este grupo de reglas en su ACL web. AWS WAF también registra las etiquetas según las CloudWatch métricas de Amazon. Para obtener información general sobre las etiquetas y las métricas de etiquetas, consulte Etiquetas en las solicitudes web y Etiquetar métricas y dimensiones.

> **Note**
>
> En esta tabla, se describe la versión estática más reciente de este grupo de reglas. Para otras versiones, usa el comando API DescribeManagedRuleGroup.

Nombre de la regla	Descripción y etiqueta
`SQLi_QUERYARGUMENTS`	Utiliza el integrado AWS WAF Instrucción de regla de ataques de inyecciones SQL, con el nivel de sensibilidad establecido enLow, para inspeccionar los valores de todos los parámetros de consulta en busca de patrones que coincidan con el código SQL malicioso. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:sql-database:SQLi_QueryArguments`
`SQLiExtendedPatterns_QUERYARGUMENTS`	Inspecciona los valores de todos los parámetros de consulta en busca de patrones que coincidan con código SQL malicioso. La regla `SQLi_QUERYARGUMENTS` no cubre los patrones que inspecciona esta regla. Acción de la regla: Block

Nombre de la regla	Descripción y etiqueta
	Etiqueta: `awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments`

Nombre de la regla	Descripción y etiqueta
`SQLi_BODY`	Utiliza el integrado AWS WAF Instrucción de regla de ataques de inyecciones SQL, con el nivel de sensibilidad establecido enLow, para inspeccionar el cuerpo de la solicitud en busca de patrones que coincidan con un código SQL malicioso. **Warning** Esta regla solo inspecciona el cuerpo de la solicitud hasta el límite de tamaño del cuerpo para la ACL web y el tipo de recurso. Para Application Load Balancer y AWS AppSync, el límite se ha fijado en 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner y Verified Access, el límite predeterminado es de 16 KB y puede aumentarlo hasta 64 KB en su configuración de ACL web. Esta regla utiliza la opción `Continue` para gestionar contenido sobredimensionado. Para obtener más información, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:sql-database:SQLi_Body`

Nombre de la regla	Descripción y etiqueta
`SQLiExtendedPatterns_BODY`	Inspecciona el cuerpo de la solicitud en busca de patrones que coincidan con el código SQL malintencionado. La regla `SQLi_BODY` no cubre los patrones que inspecciona esta regla. **Warning** Esta regla solo inspecciona el cuerpo de la solicitud hasta el límite de tamaño del cuerpo para la ACL web y el tipo de recurso. Para Application Load Balancer y AWS AppSync, el límite se ha fijado en 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner y Verified Access, el límite predeterminado es de 16 KB y puede aumentarlo hasta 64 KB en su configuración de ACL web. Esta regla utiliza la opción `Continue` para gestionar contenido sobredimensionado. Para obtener más información, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:sql-database:SQLiExtendedPatterns_Body`

Nombre de la regla	Descripción y etiqueta
`SQLi_COOKIE`	Utiliza la función integrada AWS WAF Instrucción de regla de ataques de inyecciones SQL, con el nivel de sensibilidad establecido enLow, para inspeccionar los encabezados de las cookies de las solicitudes en busca de patrones que coincidan con un código SQL malicioso. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:sql-database:SQLi_Cookie`

Grupo de reglas administrado del sistema operativo Linux

VendorName:`AWS`, Nombre:`AWSManagedRulesLinuxRuleSet`, WCU: 200

Este grupo contiene reglas que bloquean los patrones de solicitud asociados a la explotación de vulnerabilidades específicas de Linux, como 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. Tiene que valorar este grupo de reglas si alguna parte de su aplicación se ejecuta en Linux. Tiene que utilizar este grupo de reglas junto con el grupo de reglas Sistema operativo POSIX.

Este grupo de reglas administrado agrega etiquetas a las solicitudes web que evalúa, que están disponibles para las reglas que se ejecutan después de este grupo de reglas en su ACL web. AWS WAF también registra las etiquetas según las CloudWatch métricas de Amazon. Para obtener información general sobre las etiquetas y las métricas de etiquetas, consulte Etiquetas en las solicitudes web y Etiquetar métricas y dimensiones.

> **Note**
>
> En esta tabla, se describe la versión estática más reciente de este grupo de reglas. Para otras versiones, usa el comando API DescribeManagedRuleGroup.

Nombre de la regla	Descripción y etiqueta
`LFI_URIPATH`	Inspecciona la ruta de solicitud en busca de intentos de explotar las vulnerabilidades de inclusión de archivos locales (LFI) en las aplicaciones web. Los patrones de ejemplo incluyen archivos como `/proc/version` , que podrían proporcionar información del sistema operativo a los atacantes. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:linux-os:LFI_URIPath`
`LFI_QUERYSTRING`	Inspecciona los valores de todas las cadenas de la solicitud en busca de intentos de explotar las vulnerabilidades de inclusión de archivos locales (LFI) en las aplicaciones web. Los patrones de ejemplo incluyen archivos como `/proc/version` , que podrían proporcio nar información del sistema operativo a los atacantes. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:linux-os:LFI_QueryString`
`LFI_HEADER`	Inspecciona los encabezados de la en busca de intentos de explotar las vulnerabilidades de inclusión de archivos locales (LFI) en las aplicaciones web. Los patrones de ejemplo incluyen archivos como `/proc/version` , que podrían proporcionar información del sistema operativo a los atacantes.

Nombre de la regla	Descripción y etiqueta
	Warning Esta regla solo inspecciona los primeros 8 KB de encabezados de solicitudes o los primeros 200 encabezados, el límite que se alcance primero, y utiliza la opción `Continue` para gestionar contenido de gran tamaño. Para obtener más informaci ón, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:linux-os:LFI_Header`

Grupo de reglas administrado para el sistema operativo POSIX

VendorName:`AWS`, Nombre:, WCU: `AWSManagedRulesUnixRuleSet` 100

Este grupo contiene reglas que bloquean los patrones de solicitud asociados a la explotación de vulnerabilidades específicas de POSIX y de sistemas operativos similares a este, como los ataques de inclusión de archivos locales (LFI). Este puede ayudar a evitar ataques que expongan el contenido de un archivos o que ejecuten código que, en principio, tendría que ser inaccesible para los atacantes. Tiene que valorar este grupo de reglas si alguna parte de su aplicación se ejecuta en un sistema operativo POSIX o similar a POSIX, entre los que se incluyen Linux, AIX, HP-UX, macOS, Solaris, FreeBSD y OpenBSD.

Este grupo de reglas administrado agrega etiquetas a las solicitudes web que evalúa, que están disponibles para las reglas que se ejecutan después de este grupo de reglas en su ACL web. AWS WAF también registra las etiquetas según las CloudWatch métricas de Amazon. Para obtener

información general sobre las etiquetas y las métricas de etiquetas, consulte Etiquetas en las solicitudes web y Etiquetar métricas y dimensiones.

> **Note**
>
> En esta tabla, se describe la versión estática más reciente de este grupo de reglas. Para otras versiones, usa el comando API DescribeManagedRuleGroup.

Nombre de la regla	Descripción y etiqueta
`UNIXShellCommandsVariables_QUERYSTRING`	Inspecciona los valores de la cadena de consulta para detectar intentos de aprovechar las vulnerabilidades de inyección de comandos, LFI y cruce de rutas en aplicaciones web que se ejecutan en sistemas Unix. Algunos ejemplos incluyen patrones como `echo $HOME` y `echo $PATH`. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString`
`UNIXShellCommandsVariables_BODY`	Inspecciona el cuerpo de la solicitud en busca de intentos de explotar las vulnerabilidades de inyección de comandos, LFI y recorrido de ruta en aplicaciones web que se ejecutan en sistemas Unix. Algunos ejemplos incluyen patrones como `echo $HOME` y `echo $PATH`. **Warning** Esta regla solo inspecciona el cuerpo de la solicitud hasta el límite de tamaño

Nombre de la regla	Descripción y etiqueta
	del cuerpo para la ACL web y el tipo de recurso. Para Application Load Balancer y AWS AppSync, el límite se ha fijado en 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner y Verified Access, el límite predeterminado es de 16 KB y puede aumentarlo hasta 64 KB en su configuración de ACL web. Esta regla utiliza la opción `Continue` para gestionar contenido sobredimensionado. Para obtener más información, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_Body`

Nombre de la regla	Descripción y etiqueta
`UNIXShellCommandsVariables_HEADER`	Inspecciona todos los encabezados de las solicitudes para detectar intentos de aprovechar las vulnerabilidades de inyección de comandos, LFI y cruce de rutas en aplicaciones web que se ejecutan en sistemas Unix. Algunos ejemplos incluyen patrones como `echo $HOME` y `echo $PATH`. **Warning** Esta regla solo inspecciona los primeros 8 KB de encabezados de solicitudes o los primeros 200 encabezados, el límite que se alcance primero, y utiliza la opción `Continue` para gestionar contenido de gran tamaño. Para obtener más información, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_Header`

Grupo de reglas administrado para el sistema operativo Windows

VendorName:`AWS`, Nombre:`AWSManagedRulesWindowsRuleSet`, WCU: 200

El grupo de reglas del sistema operativo Windows contiene reglas que bloquean los patrones de solicitud asociados con la explotación de vulnerabilidades específicas de Windows, como

la ejecución remota de PowerShell comandos. Este puede ayudar a evitar la explotación de vulnerabilidades que permiten a un atacante ejecutar comandos no autorizados o ejecutar código malintencionado. Valore este grupo de reglas si alguna parte de la aplicación se ejecuta en un sistema operativo Windows.

Este grupo de reglas administrado agrega etiquetas a las solicitudes web que evalúa, que están disponibles para las reglas que se ejecutan después de este grupo de reglas en la ACL web. AWS WAF también registra las etiquetas según las CloudWatch métricas de Amazon. Para obtener información general sobre las etiquetas y las métricas de etiquetas, consulte Etiquetas en las solicitudes web y Etiquetar métricas y dimensiones.

> **Note**
>
> En esta tabla, se describe la versión estática más reciente de este grupo de reglas. Para otras versiones, usa el comando API DescribeManagedRuleGroup.

Nombre de la regla	Descripción y etiqueta
`WindowsShellCommands_COOKIE`	Inspecciona los encabezados de las cookies de solicitud para detectar intentos de inyección de WindowsShell comandos en aplicaciones web. Los patrones de coincidencia represent an WindowsShell comandos. Los patrones de ejemplo incluyen `||nslookup` y `;cmd`. Acción de la regla: Block Etiqueta: `awswaf:managed:aws :windows-os:WindowsShellCom mands_Cookie`
`WindowsShellCommands_QUERYA RGUMENTS`	Inspecciona los valores de todos los parámetro s de consulta para detectar intentos de inyección de WindowsShell comandos en aplicaciones web. Los patrones de coinciden cia representan WindowsShell comandos. Los

Nombre de la regla	Descripción y etiqueta
	patrones de ejemplo incluyen `||nslookup` y `;cmd`. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:windows-os:WindowsShellCommands_QueryArguments`

Nombre de la regla	Descripción y etiqueta
`WindowsShellCommands_BODY`	Inspecciona el cuerpo de la solicitud para detectar intentos de inyección de WindowsShell comandos en aplicaciones web. Los patrones de coincidencia representan WindowsShell comandos. Los patrones de ejemplo incluyen `||nslookup y ;cmd`. **Warning** Esta regla solo inspecciona el cuerpo de la solicitud hasta el límite de tamaño del cuerpo para la ACL web y el tipo de recurso. Para Application Load Balancer y AWS AppSync, el límite se ha fijado en 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner y Verified Access, el límite predeterminado es de 16 KB y puede aumentarlo hasta 64 KB en su configuración de ACL web. Esta regla utiliza la opción `Continue` para gestionar contenido sobredimensionado. Para obtener más información, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:windows-os:WindowsShellCommands_Body`

Nombre de la regla	Descripción y etiqueta
`PowerShellCommands_COOKIE`	Inspecciona los encabezados de las cookies de solicitud para detectar intentos de inyección de PowerShell comandos en aplicaciones web. Los patrones de coincidencia representan PowerShell comandos. Por ejemplo, `Invoke-Expression` . Acción de la regla: Block Etiqueta: `awswaf:managed:aws:windows-os:PowerShellCommands_Cookie`
`PowerShellCommands_QUERYARGUMENTS`	Inspecciona los valores de todos los parámetros de consulta para detectar intentos de inyección de PowerShell comandos en aplicaciones web. Los patrones de coincidencia representan PowerShell comandos. Por ejemplo, `Invoke-Expression` . Acción de la regla: Block Etiqueta: `awswaf:managed:aws:windows-os:PowerShellCommands_QueryArguments`

Nombre de la regla	Descripción y etiqueta
`PowerShellCommands_BODY`	Inspecciona el cuerpo de la solicitud para detectar intentos de inyección de PowerShell comandos en aplicaciones web. Los patrones de coincidencia representan PowerShel l comandos. Por ejemplo, `Invoke-Ex pression` . **Warning** Esta regla solo inspecciona el cuerpo de la solicitud hasta el límite de tamaño del cuerpo para la ACL web y el tipo de recurso. Para Application Load Balancer y AWS AppSync, el límite se ha fijado en 8 KB. Para CloudFron t API Gateway, Amazon Cognito, App Runner y Verified Access, el límite predeterminado es de 16 KB y puede aumentarlo hasta 64 KB en su configuración de ACL web. Esta regla utiliza la opción `Continue` para gestionar contenido sobredime nsionado. Para obtener más informaci ón, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block Etiqueta: `awswaf:managed:aws :windows-os:PowerShellComma nds_Body`

Grupo de reglas administrado de la aplicación PHP

VendorName:`AWS`, Nombre:`AWSManagedRulesPHPRuleSet`, WCU: 100

Este grupo contiene reglas que bloquean los patrones de solicitud asociados a la explotación de vulnerabilidades específicas para el uso del lenguaje de programación PHP, como la inyección de funciones PHP poco seguras. Este puede ayudar a evitar la explotación de vulnerabilidades que permiten a un atacante ejecutar de forma remota código o comandos sin autorización. Evalúe este grupo de reglas si PHP está instalado en cualquier servidor con el que interactúe su aplicación.

Este grupo de reglas administrado agrega etiquetas a las solicitudes web que evalúa, que están disponibles para las reglas que se ejecutan después de este grupo de reglas en su ACL web. AWS WAF también registra las etiquetas según las CloudWatch métricas de Amazon. Para obtener información general sobre las etiquetas y las métricas de etiquetas, consulte Etiquetas en las solicitudes web y Etiquetar métricas y dimensiones.

> **Note**
>
> En esta tabla, se describe la versión estática más reciente de este grupo de reglas. Para otras versiones, usa el comando API DescribeManagedRuleGroup.

Nombre de la regla	Descripción y etiqueta
`PHPHighRiskMethodsVariables_HEADER`	Inspecciona todos los encabezados para buscar los intentos de inyección de código de script PHP. Los patrones de ejemplo incluyen funciones como `fsockopen` y la variable superglobal `$_GET`. **Warning** Esta regla solo inspecciona los primeros 8 KB de encabezados de solicitudes o los primeros 200 encabezados, el límite que se alcance primero, y utiliza la opción `Continue` para gestionar contenido de gran

Nombre de la regla	Descripción y etiqueta
	tamaño. Para obtener más información, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Header`
`PHPHighRiskMethodsVariables_QUERYSTRING`	Inspecciona todo lo que aparece después del primer ? en la URL de la solicitud y busca intentos de inyección de código en un script PHP. Los patrones de ejemplo incluyen funciones como `fsockopen` y la variable superglobal `$_GET`. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_QueryString`

Nombre de la regla	Descripción y etiqueta
`PHPHighRiskMethodsVariables_BODY`	Inspecciona los valores del cuerpo de la solicitud para los intentos de inyección de código de script PHP. Los patrones de ejemplo incluyen funciones como `fsockopen` y la variable superglobal `$_GET`. **Warning** Esta regla solo inspecciona el cuerpo de la solicitud hasta el límite de tamaño del cuerpo para la ACL web y el tipo de recurso. Para Application Load Balancer y AWS AppSync, el límite se ha fijado en 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner y Verified Access, el límite predeterminado es de 16 KB y puede aumentarlo hasta 64 KB en su configuración de ACL web. Esta regla utiliza la opción `Continue` para gestionar contenido sobredimensionado. Para obtener más información, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Body`

WordPress grupo de reglas gestionado por aplicaciones

VendorName:`AWS`, Nombre:`AWSManagedRulesWordPressRuleSet`, WCU: 100

El grupo de reglas de la WordPress aplicación contiene reglas que bloquean los patrones de solicitud asociados a la explotación de vulnerabilidades específicas de los WordPress sitios. Si está corriendo, debe evaluar este grupo de reglasWordPress. Este grupo de reglas debe utilizarse junto con los grupos de reglas Base de datos SQL y Aplicaciones PHP.

Este grupo de reglas administrado agrega etiquetas a las solicitudes web que evalúa, que están disponibles para las reglas que se ejecutan después de este grupo de reglas en su ACL web. AWS WAF también registra las etiquetas según las CloudWatch métricas de Amazon. Para obtener información general sobre las etiquetas y las métricas de etiquetas, consulte Etiquetas en las solicitudes web y Etiquetar métricas y dimensiones.

> **Note**
>
> En esta tabla, se describe la versión estática más reciente de este grupo de reglas. Para otras versiones, usa el comando API DescribeManagedRuleGroup.

Nombre de la regla	Descripción y etiqueta
`WordPressExploitableCommands_QUERYSTRING`	Inspecciona la cadena de consulta de la solicitud para detectar WordPress comandos de alto riesgo que puedan explotarse en instalaciones o complementos vulnerables. Ejemplos de patrones incluyen comandos como `do-reset-wordpress` . Acción de la regla: Block Etiqueta: `awswaf:managed:aws:wordpress-app:WordPressExploitableCommands_QUERYSTRING`
`WordPressExploitablePaths_URIPATH`	Inspecciona la ruta del URI de la solicitud en busca de WordPress archivos como

Nombre de la regla	Descripción y etiqueta
	`xmlrpc.php` los que se sabe que tienen vulnerabilidades que se pueden explotar fácilmente. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:wordpress-app:WordPressExploitablePaths_URIPATH`

Grupos de reglas de reputación de IP

Estos grupos bloquean solicitudes en función de su dirección IP de origen.

> **Note**
>
> Estas reglas utilizan la dirección IP de origen del origen de la solicitud web. Si el tráfico pasa por uno o más proxies o equilibradores de carga, el origen de la solicitud web contendrá la dirección del último proxy y no la dirección de origen del cliente.

Elija uno o más de estos grupos de reglas si quiere reducir su exposición al tráfico de bots o los intentos de explotación o si está aplicando restricciones geográficas a su contenido. Para obtener información sobre la administración de bots, consulte también AWS WAF Grupo de reglas de control de bots.

Los grupos de reglas de esta categoría no proporcionan notificaciones de control de versiones ni de actualizaciones de SNS.

> **Note**
>
> La información que publicamos sobre las reglas de los grupos de reglas de reglas AWS administradas tiene por objeto proporcionarle información suficiente para utilizarlas, pero no proporciona información que los delincuentes puedan utilizar para eludirlas. Si necesita más información de la que se encuentra en esta documentación, póngase en contacto con el centro de AWS Support.

Grupo de reglas administrado con lista de reputación de IP de Amazon

VendorName:`AWS`, Nombre:`AWSManagedRulesAmazonIpReputationList`, WCU: 25

El grupo de reglas de la lista de reputación de IP de Amazon contiene reglas basadas en la inteligencia de amenazas interna de Amazon. Es útil si quiere bloquear direcciones IP normalmente asociadas a 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.

Este grupo de reglas administrado agrega etiquetas a las solicitudes web que evalúa, que están disponibles para las reglas que se ejecutan después de este grupo de reglas en su ACL web. AWS WAF también registra las etiquetas según las CloudWatch métricas de Amazon. Para obtener información general sobre las etiquetas y las métricas de etiquetas, consulte Etiquetas en las solicitudes web y Etiquetar métricas y dimensiones.

Nombre de la regla	Descripción y etiqueta
`AWSManagedIPReputationList`	Inspecciona las direcciones IP que se hayan identificado como implicadas activamente en actividades maliciosas. AWS WAF recopila la lista de direcciones IP de varias fuentes MadPot, incluida una herramienta de inteligen cia de amenazas que Amazon utiliza para proteger a los clientes de la ciberdelincuencia. Para obtener más información al respecto MadPot, consultehttps://www.aboutamazon.com/news/aws/amazon-madpot-stops-cybersecurity-crime. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:amazon-ip-list:AWSManagedIPReputationList`
`AWSManagedReconnaissanceList`	Inspecciona las conexiones de las direccion es IP que realizan un reconocimiento de los recursos de AWS .

Nombre de la regla	Descripción y etiqueta
	Acción de la regla: Block Etiqueta: `awswaf:managed:aws:amazon-ip-list:AWSManagedReconnaissanceList`
`AWSManagedIPDDoSList`	Inspecciona las direcciones IP que, según se ha identificado, participan activamente en actividades de DDoS. Acción de la regla: Count Etiqueta: `awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList`

Grupo de reglas administrado con lista de direcciones IP anónimas

VendorName:`AWS`, Nombre:`AWSManagedRulesAnonymousIpList`, WCU: 50

El grupo de reglas de lista de IP anónimas contiene reglas para bloquear las solicitudes de los servicios que permiten ocultar la identidad del visor. Entre estas se incluyen solicitudes de la VPN, proxies, nodos Tor y proveedores de alojamiento web. 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.

Este grupo de reglas administrado agrega etiquetas a las solicitudes web que evalúa, que están disponibles para las reglas que se ejecutan después de este grupo de reglas en su ACL web. AWS WAF también registra las etiquetas según las CloudWatch métricas de Amazon. Para obtener información general sobre las etiquetas y las métricas de etiquetas, consulte Etiquetas en las solicitudes web y Etiquetar métricas y dimensiones.

Nombre de la regla	Descripción y etiqueta
`AnonymousIPList`	Inspecciona una lista de direcciones IP de fuentes conocidas para anonimizar la informaci

Nombre de la regla	Descripción y etiqueta
	ón del cliente, como nodos TOR, proxies temporales y otros servicios de enmascara miento. Acción de la regla: Block Etiqueta: `awswaf:managed:aws :anonymous-ip-list:Anonymou sIPList`
`HostingProviderIPList`	Inspecciona la lista de direcciones IP de proveedores de alojamiento web y nube, que tienen menos probabilidades de generar tráfico de usuario final. La lista de IP no incluye direcciones AWS IP. Acción de la regla: Block Etiqueta: `awswaf:managed:aws :anonymous-ip-list:HostingP roviderIPList`

AWS WAF Grupo de reglas de prevención del fraude (ACFP) para la creación de cuentas de Control de Fraude

VendorName:`AWS`, Nombre:`AWSManagedRulesACFPRuleSet`, WCU: 50

La Oficina de Prevención del AWS WAF Fraude para la creación de cuentas (ACFP) gestionó los grupos de reglas, etiquetó los grupos de reglas y gestionó las solicitudes que pudieran formar parte de intentos fraudulentos de creación de cuentas. Para ello, el grupo de reglas inspecciona las solicitudes de creación de cuentas que los clientes envían a los puntos de conexión de registro y creación de cuentas de la aplicación.

El grupo de reglas de la ACFP inspecciona los intentos de creación de cuentas de varias maneras para ofrecerte visibilidad y control sobre posibles interacciones maliciosas. El grupo de reglas utiliza los tokens de solicitud para recopilar información sobre el navegador del cliente y sobre el nivel de interactividad humana a la hora de crear la solicitud de creación de cuentas. El grupo de

reglas detecta y gestiona los intentos de creación masiva de cuentas mediante la agregación de las solicitudes por dirección IP y sesión del cliente, y por la información de la cuenta proporcionada, como la dirección física y el número de teléfono. Además, el grupo de reglas detecta y bloquea la creación de nuevas cuentas con credenciales que se han visto comprometidas, lo que ayuda a proteger la posición de seguridad de la aplicación y de los nuevos usuarios.

Consideraciones sobre el uso de este grupo de reglas

Este grupo de reglas requiere una configuración personalizada, que incluye la especificación de las rutas de registro de cuenta y creación de cuenta de la aplicación. A menos que se indique lo contrario, las reglas de este grupo de reglas inspeccionan todas las solicitudes que los clientes envían a estos dos puntos de conexión. Para configurar e implementar este grupo de reglas, consulte las instrucciones en AWS WAF Control de fraude: creación de cuentas y prevención del fraude (ACFP).

> **Note**
>
> Se le cobrarán tarifas adicionales cuando utilice este grupo de reglas administrado. Para obtener más información, consulte AWS WAF Precios.

Este grupo de reglas forma parte de las protecciones de mitigación de amenazas inteligentes de AWS WAF. Para obtener más información, consulte AWS WAF mitigación inteligente de amenazas.

Para mantener sus costos bajos y asegurarse de que está gestionando el tráfico web como desea, utilice este grupo de reglas de acuerdo con las instrucciones que se indican en Las prácticas recomendadas para la mitigación inteligente de amenazas.

Este grupo de reglas no está disponible para su uso con grupos de usuarios de Amazon Cognito. No puede asociar una ACL web que utilice este grupo de reglas a un grupo de usuarios ni puede agregar este grupo de reglas a una ACL web que ya esté asociada a un grupo de usuarios.

Etiquetas agregadas por este grupo de reglas

Este grupo de reglas administrado agrega etiquetas a las solicitudes web que evalúa, que están disponibles para las reglas que se ejecutan después de este grupo de reglas en la ACL web. AWS WAF también registra las etiquetas según las CloudWatch métricas de Amazon. Para obtener información general sobre las etiquetas y las métricas de etiquetas, consulte Etiquetas en las solicitudes web y Etiquetar métricas y dimensiones.

Etiquetas de token

Este grupo de reglas utiliza la administración de AWS WAF tokens para inspeccionar y etiquetar las solicitudes web según el estado de sus AWS WAF tokens. AWS WAF usa tokens para el seguimiento y la verificación de las sesiones del cliente.

Para obtener información sobre los tókenes y su administración, consulte AWS WAF tokens de solicitud web.

Para obtener información sobre los componentes de las etiquetas que se describen aquí, consulte AWS WAF requisitos de nomenclatura y sintaxis de etiquetas.

Etiqueta de sesión de cliente

La etiqueta `awswaf:managed:token:id:`*`identifier`* contiene un identificador único que la administración de AWS WAF tokens utiliza para identificar la sesión del cliente. El identificador puede cambiar, por ejemplo, si el cliente adquiere un nuevo token después de descartar el que estaba utilizando.

> **Note**
>
> AWS WAF no informa de CloudWatch las estadísticas de Amazon para esta etiqueta.

Etiquetas de estado del token: prefijos del espacio de nombres de etiquetas

Las etiquetas de estado del token informan sobre el estado del token y de la información que contiene del desafío y del CAPTCHA.

Cada etiqueta de estado del token comienza con uno de los siguientes prefijos de espacio de nombres:

- `awswaf:managed:token:`: Se utiliza para informar sobre el estado general del token y el estado de la información del desafío del token.
- `awswaf:managed:captcha:`: Se utiliza para informar sobre el estado de la información del CAPTCHA del token.

Etiquetas de estado del token: nombres de etiquetas

Tras el prefijo, el resto de la etiqueta proporciona información detallada sobre el estado del token:

- `accepted`: El token de solicitud está presente y contiene lo siguiente:
  - Una solución válida del desafío o del CAPTCHA.
  - Una marca de tiempo vigente del desafío o del CAPTCHA.
  - Una especificación de dominio válida para la ACL web.

  Ejemplo: la etiqueta `awswaf:managed:token:accepted` indica que el token de la solicitud web tiene una solución válida y una marca temporal vigente para el desafío, así como un dominio válido.
- `rejected`: El token de solicitud está presente, pero no cumple con los criterios de aceptación.

  Junto con la etiqueta rechazada, la administración del token agrega un espacio de nombres y nombre de etiqueta personalizados para indicar el motivo.
  - `rejected:not_solved`: Al token le falta la solución del desafío o del CAPTCHA.
  - `rejected:expired`: La marca temporal del desafío o del CAPTCHA del token ha caducado, de acuerdo con los tiempos de inmunidad del token configurado en la ACL web.
  - `rejected:domain_mismatch`: El dominio del token no coincide con la configuración del dominio del token de su ACL web.
  - `rejected:invalid`— no se AWS WAF pudo leer el token indicado.

  Ejemplo: las etiquetas `awswaf:managed:captcha:rejected` y `awswaf:managed:captcha:rejected:expired` indican que la solicitud se rechazó porque la marca de tiempo del CAPTCHA del token ha superado el tiempo de inmunidad configurado en la ACL web.
- `absent`: La solicitud no contiene el token o el administrador del token no ha podido leerlo.

  Ejemplo: la etiqueta `awswaf:managed:captcha:absent` indica que la solicitud no tiene el token.

Etiquetas de ACFP

Este grupo de reglas genera etiquetas con el prefijo del espacio de nombres `awswaf:managed:aws:acfp:` seguido del espacio de nombres y el nombre de la etiqueta personalizados. El grupo de reglas puede agregar más de una etiqueta a una solicitud.

Puede recuperar todas las etiquetas de un grupo de reglas a través de la API llamando al `DescribeManagedRuleGroup`. Las etiquetas aparecen en la propiedad `AvailableLabels` de la respuesta.

Lista de reglas de prevención contra fraude en la creación de cuentas

En esta sección se enumeran las reglas de la ACFP en `AWSManagedRulesACFPRuleSet` y las etiquetas que las reglas del grupo de reglas agrega a las solicitudes web.

> **Note**
>
> La información que publicamos sobre las reglas en los grupos de reglas AWS gestionadas tiene por objeto proporcionarle información suficiente para utilizarlas, pero no proporciona información que los delincuentes puedan utilizar para eludirlas. Si necesita más información de la que se encuentra en esta documentación, póngase en contacto con el centro de AWS Support.

Todas las reglas de este grupo de reglas requieren un token de solicitud web, excepto las dos primeras `UnsupportedCognitoIDP` y `AllRequests`. Para obtener una descripción de la información que proporciona el token, consulte AWS WAF características del token.

A menos que se indique lo contrario, las reglas de este grupo de reglas inspeccionan todas las solicitudes que sus clientes envían a las rutas de las páginas de registro y creación de cuentas que proporcione en la configuración del grupo de reglas. Para obtener información acerca de cómo configurar este grupo de reglas, consulte AWS WAF Control de fraude: creación de cuentas y prevención del fraude (ACFP).

Nombre de la regla	Descripción y etiqueta
`UnsupportedCognitoIDP`	Inspecciona el tráfico web que se dirige a un grupo de usuarios de Amazon Cognito. La ACFP no está disponible para su uso con los grupos de usuarios de Amazon Cognito y esta regla ayuda a garantizar que las demás reglas del grupo de reglas de la ACFP no se utilicen para evaluar el tráfico del grupo de usuarios.

Nombre de la regla	Descripción y etiqueta
	Acción de la regla: Block Etiqueta: `awswaf:managed:aws:acfp:unsupported:cognito_idp`
`AllRequests`	Aplica la acción de regla a las solicitudes que acceden a la ruta de la página de registro. La ruta de la página de registro se configura al configurar el grupo de reglas. De forma predeterminada, esta regla aplica el Challenge a las solicitudes. Al aplicar esta acción, la regla garantiza que el cliente adquiera un token de desafío antes de que el resto de las reglas del grupo de reglas evalúen cualquier solicitud. Asegúrese de que los usuarios finales carguen la ruta de la página de registro antes de enviar una solicitud de creación de cuenta. Los tokens se agregan a las solicitudes de los SDK de integración de aplicaciones cliente y por las acciones de regla CAPTCHA y Challenge. Para la adquisición de tokens más eficiente, es muy recomendable que utilice los SDK de integración de aplicaciones. Para obtener más información, consulte AWS WAF integración de aplicaciones cliente. Acción de la regla: Challenge Etiqueta: ninguna

Nombre de la regla	Descripción y etiqueta
`RiskScoreHigh`	Inspecciona las solicitudes de creación de cuentas con direcciones IP u otros factores que se consideran muy sospechosos. Por lo general, esta evaluación se basa en varios factores que contribuyen, que se pueden ver en las etiquetas `risk_score` que el grupo de reglas agrega a la solicitud. Acción de la regla: Block Etiqueta: `awswaf:managed:aws :acfp:risk_score:high` La regla también puede aplicar etiquetas de puntuación de riesgo `medium` o `low` a la solicitud. Si AWS WAF no logra evaluar la puntuació n de riesgo de la solicitud web, la regla añade la etiqueta `awswaf:managed:aws :acfp:risk_score:evaluation _failed` Además, la regla agrega etiquetas con el espacio de nombres `awswaf:managed:aws :acfp:risk_score:contributor:` que incluyen el estado de la evaluación de la puntuación de riesgo y los resultados de los contribuyentes específicos a la puntuación de riesgo, como las evaluaciones de reputación de IP y de credenciales robadas.

Nombre de la regla	Descripción y etiqueta
`SignalCredentialCompromised`	Busca en la base de datos de credenciales robadas las credenciales que se enviaron en la solicitud de creación de la cuenta. Esta regla garantiza que los nuevos clientes inicialicen sus cuentas con una postura de seguridad positiva. **Note** Puede agregar una respuesta de bloqueo personalizada para describir el problema al usuario final e indicarle cómo proceder. Para obtener más información, consulte Ejemplo de ACFP: respuesta personalizada para credenciales comprometidas. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:acfp:signal:credential_compromised` El grupo de reglas aplica la siguiente etiqueta relacionada, pero no realiza ninguna acción al respecto, ya que no todas las solicitudes de creación de cuentas tendrán credencia les: `awswaf:managed:aws:acfp:signal:missing_credential`

Nombre de la regla	Descripción y etiqueta
`SignalClientHumanInteractivityAbsentLow`	Inspecciona el token de la solicitud de creación de la cuenta en busca de datos que indiquen una interactividad humana anómala con la aplicación. La interactividad humana se detecta mediante interacciones como los movimientos del ratón y las pulsaciones de teclas. Si la página tiene un formulario HTML, la interactividad humana incluye las interacciones con el formulario. **Note** Esta regla solo inspecciona las solicitudes de la ruta de creación de cuentas y solo se evalúa si ha implementado los SDK de integración de aplicaciones. Las implementaciones de los SDK capturan de forma pasiva la interactividad humana y almacenan la información en el token de solicitud. Para obtener más información, consulte AWS WAF características del token y AWS WAF integración de aplicaciones cliente. Acción de la regla: CAPTCHA Etiqueta: ninguna. La regla determina una coincidencia según diversos factores, por lo que no existe una etiqueta individual que se aplique a todos los escenarios de coincidencia posibles.

Nombre de la regla	Descripción y etiqueta
	El grupo de reglas puede aplicar una o varias de las siguientes etiquetas a las solicitudes: `awswaf:managed:aws:acfp:signal:client:human_interactivity:low/medium/high` `awswaf:managed:aws:acfp:signal:client:human_interactivity:insufficient_data` `awswaf:managed:aws:acfp:signal:form_detected` .
`SignalAutomatedBrowser`	Inspecciona la solicitud en busca de indicadores de que el navegador del cliente podría estar automatizado. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:acfp:signal:automated_browser`
`SignalBrowserInconsistency`	Inspecciona el token de la solicitud para detectar datos de interrogación del navegador incoherentes. Para obtener más información, consulte AWS WAF características del token. Acción de la regla: CAPTCHA Etiqueta: `awswaf:managed:aws:acfp:signal:browser_inconsistency`

Nombre de la regla	Descripción y etiqueta
`VolumetricIpHigh`	Comprueba si hay grandes volúmenes de solicitudes de creación de cuentas enviadas desde direcciones IP individuales. Un volumen elevado son más de 20 solicitudes en un período de 10 minutos. **Note** Los umbrales a los que se aplica esta regla pueden variar ligeramente debido a la latencia. En el caso de un volumen elevado, es posible que algunas solicitudes superen el límite antes de que se aplique la acción de regla. Acción de la regla: CAPTCHA Etiqueta: `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:high` La regla aplica las siguientes etiquetas a las solicitudes con volúmenes medios (de 16 a 20 solicitudes en un intervalo de 10 minutos) y de volúmenes bajos (de 11 a 15 solicitudes en un intervalo de 10 minutos), pero no realiza ninguna acción al respecto: `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:medium` y. `awswaf:managed:aws:acfp:agg`

Nombre de la regla	Descripción y etiqueta
	`regate:volumetric:ip:creation:low`

Nombre de la regla	Descripción y etiqueta
`VolumetricSessionHigh`	Inspecciona en busca de volúmenes elevados de solicitudes de creación de cuentas enviadas desde sesiones de clientes individuales. Un volumen elevado son más de 10 solicitudes en un período de 30 minutos. **Note** Los umbrales a los que se aplica esta regla pueden variar ligeramente debido a la latencia. Es posible que algunas solicitudes superen el límite antes de que se aplique la acción de la regla. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:high` El grupo de reglas aplica las siguientes etiquetas a las solicitudes con volúmenes medios (de 6 a 10 solicitudes en un intervalo de 30 minutos) y de volúmenes bajos (de 2 a 5 solicitudes en un intervalo de 30 minutos), pero no realiza ninguna acción al respecto: `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:medium` y. `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:low`

Nombre de la regla	Descripción y etiqueta
`AttributeUsernameTraversalHigh`	Comprueba si hay una alta tasa de solicitudes de creación de cuentas procedentes de una sola sesión de cliente que utilizan nombres de usuario diferentes. El límite para una evaluación alta es de más de 10 solicitudes en 30 minutos. **Note** Los umbrales a los que se aplica esta regla pueden variar ligeramente debido a la latencia. Es posible que algunas solicitudes superen el límite antes de que se aplique la acción de la regla. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:high` La regla aplica las siguientes etiquetas a las solicitudes con volúmenes medios (de 6 a 10 solicitudes en un intervalo de 30 minutos) y de volúmenes bajos (de 2 a 5 solicitudes en un intervalo de 30 minutos) de solicitudes transversales de nombre de usuario, pero no realiza ninguna acción al respecto: `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:medium` y. `awswaf:managed:aws:acfp:agg`

Nombre de la regla	Descripción y etiqueta
	`regate:attribute:username_traversal:creation:low`

Nombre de la regla	Descripción y etiqueta
`VolumetricPhoneNumberHigh`	Comprueba si hay grandes volúmenes de solicitudes de creación de cuentas que utilizan el mismo número de teléfono. El límite para una evaluación alta es de más de 10 solicitud es en 30 minutos. **Note** Los umbrales a los que se aplica esta regla pueden variar ligeramente debido a la latencia. Es posible que algunas solicitudes superen el límite antes de que se aplique la acción de la regla. Acción de la regla: Block Etiqueta: `awswaf:managed:aws :acfp:aggregate:volumetric: phone_number:high` El grupo de reglas aplica las siguientes etiquetas a las solicitudes con volúmenes medios (de 6 a 10 solicitudes en un intervalo de 30 minutos) y de volúmenes bajos (de 2 a 5 solicitudes en un intervalo de 30 minutos), pero no realiza ninguna acción al respecto: `awswaf:managed:aws:acfp:agg regate:volumetric:phone_num ber:medium` y. `awswaf:managed:aws :acfp:aggregate:volumetric: phone_number:low`

Nombre de la regla	Descripción y etiqueta
`VolumetricAddressHigh`	Comprueba si hay grandes volúmenes de solicitudes de creación de cuentas que utilizan la misma dirección física. El umbral para una evaluación alta es más de 100 solicitudes por intervalo de 30 minutos. **Note** Los umbrales a los que se aplica esta regla pueden variar ligeramente debido a la latencia. Es posible que algunas solicitudes superen el límite antes de que se aplique la acción de la regla. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:acfp:aggregate:volumetric:address:high`

Nombre de la regla	Descripción y etiqueta
`VolumetricAddressLow`	Inspecciona los volúmenes bajos y medios de solicitudes de creación de cuentas que utilizan la misma dirección física. El límite para una evaluación media es de más de 51 a 100 solicitudes por período de 30 minutos y para una evaluación baja es de 11 a 50 solicitudes por período de 30 minutos. La regla aplica la acción a volúmenes medios o bajos. **Note** Los umbrales a los que se aplica esta regla pueden variar ligeramente debido a la latencia. Es posible que algunas solicitudes superen el límite antes de que se aplique la acción de la regla. Acción de la regla: CAPTCHA Etiqueta: `awswaf:managed:aws:acfp:aggregate:volumetric:address:low` o `awswaf:managed:aws:acfp:aggregate:volumetric:address:medium`

Nombre de la regla	Descripción y etiqueta
`VolumetricIPSuccessfulResponse`	Comprueba si hay un gran volumen de solicitudes de creación de cuentas correctas para una sola dirección IP. Esta regla agrega las respuestas correctas del recurso protegido a las solicitudes de creación de cuentas. El umbral para una evaluación alta es más de 10 solicitudes por intervalo de 10 minutos. Esta regla ayuda a proteger contra los intentos de creación masiva de cuentas. Tiene un umbral inferior al de la regla `VolumetricIpHigh` , que solo cuenta las solicitudes. Si ha configurado el grupo de reglas para inspeccionar el cuerpo de la respuesta o los componentes de JSON, AWS WAF puede inspeccionar los primeros 65.536 bytes (64 KB) de estos tipos de componentes para ver si hay indicadores de éxito o error. Esta regla aplica la acción y el etiquetado de la regla a las nuevas solicitudes web desde una dirección IP, en función de las respuestas correctas y fallidas del recurso protegido a los intentos de inicio de sesión recientes desde la misma dirección IP. Al configurar el grupo de reglas, defina cómo contar los éxitos y los fracasos. **Note** AWS WAF solo evalúa esta regla en las ACL web que protegen las distribuciones de Amazon CloudFront .

Nombre de la regla	Descripción y etiqueta
	Note Los umbrales a los que se aplica esta regla pueden variar ligeramente debido a la latencia. Es posible que el cliente envíe más intentos de creación de cuentas satisfactorios de los permitidos antes de que la regla empiece a coincidir en los intentos posteriores. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:high` El grupo de reglas también aplica las siguientes etiquetas relacionadas a las solicitudes, sin ninguna acción asociada. Todos los recuentos son para un período de 10 minutos. `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:medium` para más de 5 solicitudes correctas, `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:low` para más de 1 solicitud correcta, `awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:high` para más de 10 solicitudes correctas, `awswaf:managed:aws`

Nombre de la regla	Descripción y etiqueta
	`:acfp:aggregate:volumetric:ip:failed_creation_response:medium` para más de 5 solicitudes correctas y `awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:low` para más de 1 solicitud correcta.

Nombre de la regla	Descripción y etiqueta
`VolumetricSessionSuccessful Response`	Comprueba si hay un bajo volumen de respuestas satisfactorias del recurso protegido a las solicitudes de creación de cuentas que se envían desde una sola sesión de cliente. Esto ayuda a proteger contra los intentos de creación masiva de cuentas. El umbral para una evaluación baja es más de 1 solicitud por intervalo de 30 minutos. Esto ayuda a proteger contra los intentos de creación masiva de cuentas. Esta regla usa un umbral inferior al de la regla `VolumetricSessionHigh` , que solo rastrea las solicitudes. Si ha configurado el grupo de reglas para inspeccionar el cuerpo de la respuesta o los componentes de JSON, AWS WAF puede inspeccionar los primeros 65.536 bytes (64 KB) de estos tipos de componentes para ver si hay indicadores de éxito o error. Esta regla aplica la acción y el etiquetado de la regla a las nuevas solicitudes web de una sesión de cliente, basándose en las respuesta s de éxito y fracaso del recurso protegido a los intentos de inicio de sesión recientes de la misma sesión de cliente. Al configurar el grupo de reglas, defina cómo contar los éxitos y los fracasos.

Nombre de la regla	Descripción y etiqueta
	Note AWS WAF solo evalúa esta regla en las ACL web que protegen las distribuciones de Amazon CloudFront .
	Note Los umbrales a los que se aplica esta regla pueden variar ligeramente debido a la latencia. Es posible que el cliente envíe más intentos de creación de cuentas fallidos de los permitidos antes de que la regla empiece a coincidir en los intentos posteriores.
	Acción de la regla: Block Etiqueta: `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:low` El grupo de reglas también aplica las siguientes etiquetas relacionadas a las solicitudes. Todos los recuentos son para un período de 30 minutos. `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:high` para más de 10 solicitudes correctas, `awswaf:managed:aws:acfp:aggregate:volumetric:`

Nombre de la regla	Descripción y etiqueta
	`session:successful_creation_response:medium` para más de 5 solicitud correcta, `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:high` para más de 10 solicitudes fallidas, `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:medium` para más de 5 solicitudes fallidas y `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:low` para más de 1 solicitud fallida.
`VolumetricSessionTokenReuseIp`	Inspecciona las solicitudes de creación de cuentas para detectar el uso de un único token entre más de 5 direcciones IP distintas. **Note** Los umbrales a los que se aplica esta regla pueden variar ligeramente debido a la latencia. Es posible que algunas solicitudes superen el límite antes de que se aplique la acción de la regla. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:token_reuse:ip`

AWS WAF Grupo de reglas de prevención de apropiación de cuentas (ATP) para el control del fraude

VendorName:`AWS`, Nombre:`AWSManagedRulesATPRuleSet`, WCU: 50

El sistema de prevención de apropiación de cuentas (ATP) de AWS WAF Fraud Control gestionaba las etiquetas de los grupos de reglas y gestionaba las solicitudes que podían formar parte de intentos malintencionados de apropiación de cuentas. Para ello, el grupo de reglas inspecciona los intentos de inicio de sesión que los clientes envían al punto de conexión de inicio de sesión de la aplicación.

- Inspección de solicitudes: la ATP le permite ver y controlar los intentos de inicio de sesión anómalos y los intentos de inicio de sesión que utilizan credenciales robadas con el fin de evitar la apropiación de cuentas que pueda dar lugar a actividades fraudulentas. La ATP comprueba las combinaciones de correo electrónico y contraseña con su base de datos de credenciales robadas, que se actualiza periódicamente a medida que se descubren nuevas credenciales filtradas en la web oscura. La ATP agrega los datos por dirección IP y sesión de cliente para detectar y bloquear a los clientes que envían demasiadas solicitudes de naturaleza sospechosa.
- Inspección de respuestas: en el caso de CloudFront las distribuciones, además de inspeccionar las solicitudes de inicio de sesión entrantes, el grupo de reglas de la ATP inspecciona las respuestas de la aplicación a los intentos de inicio de sesión para hacer un seguimiento de las tasas de éxito y fracaso. Con esta información, la ATP puede bloquear temporalmente las sesiones de los clientes o las direcciones IP que tengan demasiados errores de inicio de sesión. AWS WAF realiza una inspección de las respuestas de forma asíncrona, por lo que no aumenta la latencia del tráfico web.

Consideraciones sobre el uso de este grupo de reglas

Este grupo de reglas requiere una configuración específica. Para configurar e implementar este grupo de reglas, consulte las instrucciones en AWS WAF Control de fraudes y prevención de apropiación de cuentas (ATP).

Este grupo de reglas forma parte de las protecciones de mitigación de amenazas inteligentes de AWS WAF. Para obtener más información, consulte AWS WAF mitigación inteligente de amenazas.

> **Note**
>
> Se le cobrarán tarifas adicionales cuando utilice este grupo de reglas administrado. Para obtener más información, consulte AWS WAF Precios.

Para mantener sus costos bajos y asegurarse de que está gestionando el tráfico web como desea, utilice este grupo de reglas de acuerdo con las instrucciones que se indican en Las prácticas recomendadas para la mitigación inteligente de amenazas.

Este grupo de reglas no está disponible para su uso con grupos de usuarios de Amazon Cognito. No puede asociar una ACL web que utilice este grupo de reglas a un grupo de usuarios ni puede agregar este grupo de reglas a una ACL web que ya esté asociada a un grupo de usuarios.

Etiquetas agregadas por este grupo de reglas

Este grupo de reglas administrado agrega etiquetas a las solicitudes web que evalúa, que están disponibles para las reglas que se ejecutan después de este grupo de reglas en la ACL web. AWS WAF también registra las etiquetas según las CloudWatch métricas de Amazon. Para obtener información general sobre las etiquetas y las métricas de etiquetas, consulte Etiquetas en las solicitudes web y Etiquetar métricas y dimensiones.

Etiquetas de token

Este grupo de reglas utiliza la administración de AWS WAF tokens para inspeccionar y etiquetar las solicitudes web según el estado de sus AWS WAF tokens. AWS WAF usa tokens para el seguimiento y la verificación de las sesiones del cliente.

Para obtener información sobre los tókenes y su administración, consulte AWS WAF tokens de solicitud web.

Para obtener información sobre los componentes de las etiquetas que se describen aquí, consulte AWS WAF requisitos de nomenclatura y sintaxis de etiquetas.

Etiqueta de sesión de cliente

La etiqueta `awswaf:managed:token:id:`*`identifier`* contiene un identificador único que la administración de AWS WAF tokens utiliza para identificar la sesión del cliente. El identificador puede cambiar, por ejemplo, si el cliente adquiere un nuevo token después de descartar el que estaba utilizando.

> **Note**
>
> AWS WAF no informa de CloudWatch las estadísticas de Amazon para esta etiqueta.

Etiquetas de estado del token: prefijos del espacio de nombres de etiquetas

Las etiquetas de estado del token informan sobre el estado del token y de la información que contiene del desafío y del CAPTCHA.

Cada etiqueta de estado del token comienza con uno de los siguientes prefijos de espacio de nombres:

- `awswaf:managed:token:`: Se utiliza para informar sobre el estado general del token y el estado de la información del desafío del token.
- `awswaf:managed:captcha:`: Se utiliza para informar sobre el estado de la información del CAPTCHA del token.

Etiquetas de estado del token: nombres de etiquetas

Tras el prefijo, el resto de la etiqueta proporciona información detallada sobre el estado del token:

- `accepted`: El token de solicitud está presente y contiene lo siguiente:
  - Una solución válida del desafío o del CAPTCHA.
  - Una marca de tiempo vigente del desafío o del CAPTCHA.
  - Una especificación de dominio válida para la ACL web.

  Ejemplo: la etiqueta `awswaf:managed:token:accepted` indica que el token de la solicitud web tiene una solución válida y una marca temporal vigente para el desafío, así como un dominio válido.
- `rejected`: El token de solicitud está presente, pero no cumple con los criterios de aceptación.

  Junto con la etiqueta rechazada, la administración del token agrega un espacio de nombres y nombre de etiqueta personalizados para indicar el motivo.
  - `rejected:not_solved`: Al token le falta la solución del desafío o del CAPTCHA.
  - `rejected:expired`: La marca temporal del desafío o del CAPTCHA del token ha caducado, de acuerdo con los tiempos de inmunidad del token configurado en la ACL web.
  - `rejected:domain_mismatch`: El dominio del token no coincide con la configuración del dominio del token de su ACL web.
  - `rejected:invalid`— no se AWS WAF pudo leer el token indicado.

  Ejemplo: las etiquetas `awswaf:managed:captcha:rejected` y `awswaf:managed:captcha:rejected:expired` indican que la solicitud se rechazó porque la

marca de tiempo del CAPTCHA del token ha superado el tiempo de inmunidad configurado en la ACL web.

- `absent`: La solicitud no contiene el token o el administrador del token no ha podido leerlo.

  Ejemplo: la etiqueta `awswaf:managed:captcha:absent` indica que la solicitud no tiene el token.

Etiquetas de ATP

Este grupo de reglas administrado por ATP genera etiquetas con el prefijo del espacio de nombres `awswaf:managed:aws:atp:` seguido del espacio de nombres y el nombre de la etiqueta personalizados.

El grupo de reglas puede agregar cualquiera de las siguientes etiquetas además de las que aparecen en la lista de reglas:

- `awswaf:managed:aws:atp:signal:credential_compromised`: indica que las credenciales que se enviaron en la solicitud se encuentran en la base de datos de credenciales robadas.
- `awswaf:managed:aws:atp:aggregate:attribute:suspicious_tls_fingerprint`— Disponible solo para CloudFront distribuciones protegidas de Amazon. Indica que la sesión de un cliente ha enviado varias solicitudes que utilizaban una huella digital de TLS sospechosa.
- `awswaf:managed:aws:atp:aggregate:volumetric:session:token_reuse:ip`: indica el uso de un único token entre más de 5 direcciones IP distintas. Los umbrales a los que se aplica esta regla pueden variar ligeramente debido a la latencia. En el caso de un volumen elevado, es posible que algunas solicitudes superen el límite antes de que se aplique la etiqueta.

Puede recuperar todas las etiquetas de un grupo de reglas a través de la API llamando al `DescribeManagedRuleGroup`. Las etiquetas aparecen en la propiedad `AvailableLabels` de la respuesta.

Lista de reglas de prevención de apropiación de cuentas

En esta sección se enumeran las reglas de la ATP en `AWSManagedRulesATPRuleSet` y las etiquetas que las reglas del grupo de reglas agrega a las solicitudes web.

> **Note**
>
> La información que publicamos sobre las reglas de los grupos de reglas AWS gestionadas tiene por objeto proporcionarle información suficiente para utilizarlas, pero no proporciona información que los delincuentes puedan utilizar para eludirlas. Si necesita más información de la que se encuentra en esta documentación, póngase en contacto con el centro de AWS Support.

Nombre de la regla	Descripción y etiqueta
`UnsupportedCognitoIDP`	Inspecciona el tráfico web que se dirige a un grupo de usuarios de Amazon Cognito. La ACFP no está disponible para su uso con los grupos de usuarios de Amazon Cognito y esta regla ayuda a garantizar que las demás reglas del grupo de reglas de la ATP no se utilicen para evaluar el tráfico del grupo de usuarios. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:atp:unsupported:cognito_idp`
`VolumetricIpHigh`	Inspecciona en busca de altos volúmenes de solicitudes enviadas desde direcciones IP individuales. Un volumen elevado son más de 20 solicitudes en un período de 10 minutos. **Note** Los umbrales a los que se aplica esta regla pueden variar ligeramente debido a la latencia. En el caso de un volumen elevado, es posible que algunas solicitudes superen el límite

Nombre de la regla	Descripción y etiqueta
	antes de que se aplique la acción de regla. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:atp:aggregate:volumetric:ip:high` El grupo de reglas aplica las siguientes etiquetas a las solicitudes con volúmenes medios (de 16 a 20 solicitudes en un intervalo de 10 minutos) y de volúmenes bajos (de 11 a 15 solicitudes en un intervalo de 10 minutos), pero no realiza ninguna acción al respecto: `awswaf:managed:aws:atp:aggregate:volumetric:ip:medium` y. `awswaf:managed:aws:atp:aggregate:volumetric:ip:low`

Nombre de la regla	Descripción y etiqueta
`VolumetricSession`	Inspecciona los grandes volúmenes de solicitud es enviadas desde las sesiones individuales de los clientes. El umbral es de más de 20 solicitudes por período de 30 minutos. Esta inspección solamente se aplica cuando la solicitud web tiene un token. Los tokens se agregan a las solicitudes por los SDK de integración de y por las acciones de regla CAPTCHA y Challenge. Para obtener más información, consulte AWS WAF tokens de solicitud web. **Note** Los umbrales a los que se aplica esta regla pueden variar ligeramente debido a la latencia. Es posible que algunas solicitudes superen el límite antes de que se aplique la acción de la regla. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:atp:aggregate:volumetric:session`

Nombre de la regla	Descripción y etiqueta
`AttributeCompromisedCredentials`	Comprueba si hay varias solicitudes de la misma sesión de cliente que utilizan credencia les robadas. Acción de la regla: Block Etiqueta: `awswaf:managed:aws :atp:aggregate:attribute:co mpromised_credentials`
`AttributeUsernameTraversal`	Comprueba si hay varias solicitudes de la misma sesión de cliente que utilizan el nombre de usuario transversal. Acción de la regla: Block Etiqueta: `awswaf:managed:aws :atp:aggregate:attribute:us ername_traversal`
`AttributePasswordTraversal`	Comprueba si hay varias solicitudes con el mismo nombre de usuario que utilizan el barrido de contraseñas. Acción de la regla: Block Etiqueta: `awswaf:managed:aws :atp:aggregate:attribute:pa ssword_traversal`

Nombre de la regla	Descripción y etiqueta
`AttributeLongSession`	Comprueba si hay varias solicitudes de la misma sesión de cliente que utilizan sesiones largas. Esta inspección solamente se aplica cuando la solicitud web tiene un token. Los tokens se agregan a las solicitudes por los SDK de integración de y por las acciones de regla CAPTCHA y Challenge. Para obtener más información, consulte AWS WAF tokens de solicitud web. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:atp:aggregate:attribute:long_session`

Nombre de la regla	Descripción y etiqueta
`TokenRejected`	Inspecciona las solicitudes con fichas que la administración de las mismas ha rechazado AWS WAF . Esta inspección solamente se aplica cuando la solicitud web tiene un token. Los tokens se agregan a las solicitudes por los SDK de integración de y por las acciones de regla CAPTCHA y Challenge. Para obtener más información, consulte AWS WAF tokens de solicitud web. Acción de la regla: Block Etiqueta: ninguna. Para comprobar si el token ha sido rechazado, utiliza una regla de coincidencia de etiquetas para que coincida con la etiqueta: `awswaf:managed:token:rejected`
`SignalMissingCredential`	Inspecciona las solicitudes con credenciales a las que les falte el nombre de usuario o la contraseña. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:atp:signal:missing_credential`

Nombre de la regla	Descripción y etiqueta
`VolumetricIpFailedLoginResponseHigh`	Comprueba si hay direcciones IP que hayan originado recientemente una tasa demasiado alta de intentos fallidos de inicio de sesión. Un volumen elevado son más de 10 solicitudes de inicio de sesión fallidas desde una dirección IP en un período de 10 minutos. Si ha configurado el grupo de reglas para inspeccionar el cuerpo de la respuesta o los componentes de JSON, AWS WAF puede inspeccionar los primeros 65.536 bytes (64 KB) de estos tipos de componentes para ver si hay indicadores de éxito o error. Esta regla aplica la acción y el etiquetado de la regla a las nuevas solicitudes web desde una dirección IP, en función de las respuesta s correctas y fallidas del recurso protegido a los intentos de inicio de sesión recientes desde la misma dirección IP. Al configurar el grupo de reglas, defina cómo contar los éxitos y los fracasos. **Note** AWS WAF solo evalúa esta regla en las ACL web que protegen las distribuc iones de Amazon CloudFront. **Note** Los umbrales a los que se aplica esta regla pueden variar ligeramente debido

Nombre de la regla	Descripción y etiqueta
	a la latencia. Es posible que el cliente envíe más intentos de inicio de sesión de los permitidos antes de que la regla empiece a coincidir en los intentos posteriores. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high` El grupo de reglas también aplica las siguientes etiquetas relacionadas a las solicitudes, sin ninguna acción asociada. Todos los recuentos son para un período de 10 minutos. `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:medium` para más de 5 solicitudes correctas, `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:low` para más de 1 solicitud fallida, `awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:high` para más de 10 solicitudes correctas, `awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:medium` para más de 5 solicitudes correctas y `awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:low` para más de 1 solicitud correcta.

Nombre de la regla	Descripción y etiqueta

Nombre de la regla	Descripción y etiqueta
`VolumetricSessionFailedLogi nResponseHigh`	Comprueba si hay sesiones de cliente que hayan originado recientemente una tasa demasiado alta de intentos de inicio de sesión fallidos. Un volumen elevado son más de 10 solicitudes de inicio de sesión fallidas desde una sesión de cliente en un período de 30 minutos. Si ha configurado el grupo de reglas para inspeccionar el cuerpo de la respuesta o los componentes de JSON, AWS WAF puede inspeccionar los primeros 65.536 bytes (64 KB) de estos tipos de componentes para ver si hay indicadores de éxito o error. Esta regla aplica la acción y el etiquetado de la regla a las nuevas solicitudes web de una sesión de cliente, basándose en las respuesta s de éxito y fracaso del recurso protegido a los intentos de inicio de sesión recientes de la misma sesión de cliente. Al configurar el grupo de reglas, defina cómo contar los éxitos y los fracasos. **Note** AWS WAF solo evalúa esta regla en las ACL web que protegen las distribuc iones de Amazon CloudFront .

Nombre de la regla	Descripción y etiqueta
	Note Los umbrales a los que se aplica esta regla pueden variar ligeramente debido a la latencia. Es posible que el cliente envíe más intentos de inicio de sesión de los permitidos antes de que la regla empiece a coincidir en los intentos posteriores. Esta inspección solamente se aplica cuando la solicitud web tiene un token. Los tokens se agregan a las solicitudes por los SDK de integración de y por las acciones de regla CAPTCHA y Challenge. Para obtener más información, consulte AWS WAF tokens de solicitud web. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:high` El grupo de reglas también aplica las siguientes etiquetas relacionadas a las solicitudes, sin ninguna acción asociada. Todos los recuentos son para un período de 30 minutos. `awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:medium` para más de 5 solicitudes correctas, `awswaf:managed:aws:atp:aggregate:vol`

Nombre de la regla	Descripción y etiqueta
	`umetric:session:failed_logi n_response:low` para más de 1 solicitud fallida, `awswaf:managed:aws:atp:aggr egate:volumetric:session:su ccessful_login_response:hig h` para más de 10 solicitudes correctas , `awswaf:managed:aws:atp:aggr egate:volumetric:session:su ccessful_login_response:med ium` para más de 5 solicitudes correctas y `awswaf:managed:aws:atp:aggr egate:volumetric:session:su ccessful_login_response:low` para más de 1 solicitud correcta.

AWS WAF Grupo de reglas de control de bots

VendorName:`AWS`, Nombre:`AWSManagedRulesBotControlRuleSet`, WCU: 50

El grupo de reglas administrado de control de bots proporciona reglas que gestionan las solicitudes de los bots. Los bots pueden consumir un exceso de recursos, distorsionar las métricas empresariales, provocar tiempos de inactividad y realizar actividades malintencionadas.

Niveles de protección

El grupo de reglas administrado de control de bots ofrece dos niveles de protección entre los que puede elegir:

- Común: detecta una variedad de bots que se identifican a sí mismos, como los sistemas de rastreo web, los motores de búsqueda y los navegadores automatizados. Las protecciones de control de bots de este nivel identifican los bots más comunes mediante técnicas tradicionales de detección de bots, como el análisis de datos de solicitudes estáticas. Las reglas etiquetan el tráfico de estos bots y bloquean los que no pueden verificar.
- Objetivo: incluye las protecciones de nivel común y añade una detección dirigida para los bots sofisticados que no se identifican a sí mismos. Las protecciones específicas mitigan la actividad de

los bots mediante una combinación de límites de tasas, CAPTCHA y desafíos relacionados con el navegador en segundo plano.

- **`TGT_`**: las reglas que proporcionan una protección específica tienen nombres que comienzan por `TGT_`. Todas las protecciones específicas utilizan técnicas de detección, como la interrogación del navegador, la toma de huellas digitales y la heurística del comportamiento, para identificar el tráfico de bots inapropiado.
- **`TGT_ML_`**: las reglas de protección específicas que utilizan el machine learning tienen nombres que comienzan por `TGT_ML_`. Estas reglas utilizan un análisis automatizado y de aprendizaje automático de las estadísticas de tráfico del sitio web para detectar comportamientos anómalos indicativos de una actividad de bots distribuida y coordinada. AWS WAF analiza las estadísticas sobre el tráfico de su sitio web, como las marcas horarias, las características del navegador y la URL visitada anteriormente, para mejorar el modelo de aprendizaje automático de Bot Control. Las capacidades de machine learning están habilitadas de forma predeterminada, pero puede deshabilitarlas en la configuración de su grupo de reglas. Cuando el aprendizaje automático está desactivado, AWS WAF no evalúa estas reglas.

Tanto el nivel de protección objetivo como la declaración de reglas AWS WAF basada en la velocidad proporcionan una limitación de la velocidad. Para ver una comparación de las dos opciones, consulte Opciones para limitar las tasas en las reglas basadas en tasas y en las reglas específicas de control de bots.

Consideraciones sobre el uso de este grupo de reglas

Este grupo de reglas forma parte de las protecciones de mitigación de amenazas inteligentes de AWS WAF. Para obtener más información, consulte AWS WAF mitigación inteligente de amenazas.

> **Note**
>
> Se le cobrarán tarifas adicionales cuando utilice este grupo de reglas administrado. Para obtener más información, consulte AWS WAF Precios.

Para mantener sus costos bajos y asegurarse de que está gestionando el tráfico web como desea, utilice este grupo de reglas de acuerdo con las instrucciones que se indican en Las prácticas recomendadas para la mitigación inteligente de amenazas.

Actualizamos periódicamente nuestros modelos de aprendizaje automático (ML) para adaptarlos a las reglas basadas en el aprendizaje automático con el nivel de protección específico, a fin de

mejorar las predicciones de los bots. Las reglas basadas en el aprendizaje automático tienen nombres que comienzan por. `TGT_ML_` Si observas un cambio repentino y sustancial en las predicciones de los bots según estas reglas, ponte en contacto con nosotros a través de tu administrador de cuentas o abre un caso en AWS Support Center.

Etiquetas agregadas por este grupo de reglas

Este grupo de reglas administrado agrega etiquetas a las solicitudes web que evalúa, que están disponibles para las reglas que se ejecutan después de este grupo de reglas en su ACL web. AWS WAF también registra las etiquetas según las CloudWatch métricas de Amazon. Para obtener información general sobre las etiquetas y las métricas de etiquetas, consulte Etiquetas en las solicitudes web y Etiquetar métricas y dimensiones.

Etiquetas de token

Este grupo de reglas utiliza la administración de AWS WAF tokens para inspeccionar y etiquetar las solicitudes web según el estado de sus AWS WAF tokens. AWS WAF usa tokens para el seguimiento y la verificación de las sesiones del cliente.

Para obtener información sobre los tókenes y su administración, consulte AWS WAF tokens de solicitud web.

Para obtener información sobre los componentes de las etiquetas que se describen aquí, consulte AWS WAF requisitos de nomenclatura y sintaxis de etiquetas.

Etiqueta de sesión de cliente

La etiqueta `awswaf:managed:token:id:`*`identifier`* contiene un identificador único que la administración de AWS WAF tokens utiliza para identificar la sesión del cliente. El identificador puede cambiar, por ejemplo, si el cliente adquiere un nuevo token después de descartar el que estaba utilizando.

> **Note**
>
> AWS WAF no informa de CloudWatch las estadísticas de Amazon para esta etiqueta.

Etiquetas de estado del token: prefijos del espacio de nombres de etiquetas

Las etiquetas de estado del token informan sobre el estado del token y de la información que contiene del desafío y del CAPTCHA.

Cada etiqueta de estado del token comienza con uno de los siguientes prefijos de espacio de nombres:

- `awswaf:managed:token:`: Se utiliza para informar sobre el estado general del token y el estado de la información del desafío del token.
- `awswaf:managed:captcha:`: Se utiliza para informar sobre el estado de la información del CAPTCHA del token.

Etiquetas de estado del token: nombres de etiquetas

Tras el prefijo, el resto de la etiqueta proporciona información detallada sobre el estado del token:

- `accepted`: El token de solicitud está presente y contiene lo siguiente:
  - Una solución válida del desafío o del CAPTCHA.
  - Una marca de tiempo vigente del desafío o del CAPTCHA.
  - Una especificación de dominio válida para la ACL web.

  Ejemplo: la etiqueta `awswaf:managed:token:accepted` indica que el token de la solicitud web tiene una solución válida y una marca temporal vigente para el desafío, así como un dominio válido.
- `rejected`: El token de solicitud está presente, pero no cumple con los criterios de aceptación.

  Junto con la etiqueta rechazada, la administración del token agrega un espacio de nombres y nombre de etiqueta personalizados para indicar el motivo.
  - `rejected:not_solved`: Al token le falta la solución del desafío o del CAPTCHA.
  - `rejected:expired`: La marca temporal del desafío o del CAPTCHA del token ha caducado, de acuerdo con los tiempos de inmunidad del token configurado en la ACL web.
  - `rejected:domain_mismatch`: El dominio del token no coincide con la configuración del dominio del token de su ACL web.
  - `rejected:invalid`— no se AWS WAF pudo leer el token indicado.

  Ejemplo: las etiquetas `awswaf:managed:captcha:rejected` y `awswaf:managed:captcha:rejected:expired` indican que la solicitud se rechazó porque la marca de tiempo del CAPTCHA del token ha superado el tiempo de inmunidad configurado en la ACL web.
- `absent`: La solicitud no contiene el token o el administrador del token no ha podido leerlo.

Ejemplo: la etiqueta `awswaf:managed:captcha:absent` indica que la solicitud no tiene el token.

Etiquetas de control de bots

Este grupo de reglas administrado para control de bots genera etiquetas con el prefijo del espacio de nombres `awswaf:managed:aws:bot-control:` seguido del espacio de nombres y el nombre de la etiqueta personalizados. El grupo de reglas puede agregar más de una etiqueta a una solicitud.

Cada etiqueta refleja los resultados de la regla de control de bots:

- `awswaf:managed:aws:bot-control:bot:`: información sobre el bot asociado a la solicitud.
  - `awswaf:managed:aws:bot-control:bot:name:`*`<name>`*: el nombre del bot, si hay alguno disponible, por ejemplo, los espacios de nombres personalizados `bot:name:slurp`, `bot:name:googlebot` y `bot:name:pocket_parser`.
  - `awswaf:managed:aws:bot-control:bot:category:`*`<category>`*— La categoría de bot, tal como se define AWS WAF, por ejemplo, en `bot:category:search_engine` y`bot:category:content_fetcher`.
  - `awswaf:managed:aws:bot-control:bot:organization:`*`<organization>`*: el publicador del bot, por ejemplo, `bot:organization:google`.
  - `awswaf:managed:aws:bot-control:bot:verified`: se utiliza para indicar un bot que se identifica y que el control de bots ha podido verificar. Se usa para los bots más habituales y deseables, y puede resultar útil si se combina con etiquetas de categorías como `bot:category:search_engine` o etiquetas de nombres como `bot:name:googlebot`.

> **Note**
>
> El control de bots usa la dirección IP del origen de la solicitud web para ayudar a determinar si un bot está verificado. No puedes configurarlo para que utilice la configuración de IP AWS WAF reenviada para inspeccionar una fuente de direcciones IP diferente. Si ha verificado que los bots se enrutan a través de un proxy o un equilibrador de carga, puede agregar una regla que se ejecute antes que el grupo de reglas de control de bots para ayudarle a solucionar este problema. Configura su nueva regla para usar la dirección IP reenviada y permitir de forma explícita las solicitudes de los bots

verificados. Para obtener información acerca de usar direcciones IP reenviadas, consulte Dirección IP reenviada.

- `awswaf:managed:aws:bot-control:bot:user_triggered:verified`: se utiliza para indicar un bot similar a un bot verificado, pero que los usuarios finales pueden invocar directamente. Las reglas de control de bots consideran que esta categoría de bot es un bot no verificado.
- `awswaf:managed:aws:bot-control:bot:developer_platform:verified`: se utiliza para indicar un bot similar a un bot verificado, pero que utiliza las plataformas de desarrolladores para crear scripts, por ejemplo, Google Apps Script. Las reglas de control de bots consideran que esta categoría de bot es un bot no verificado.
- `awswaf:managed:aws:bot-control:bot:unverified`: se usa para indicar un bot que se identifica a sí mismo, por lo que se le puede nombrar y clasificar, pero no publica información que pueda usarse para verificar su identidad de forma independiente. Estos tipos de firmas de bots se pueden falsificar y, por lo tanto, se consideran no verificadas.

- `awswaf:managed:aws:bot-control:targeted:<additional-details>` : se utiliza para etiquetas específicas de las protecciones específicas de control de bots.
- `awswaf:managed:aws:bot-control:signal:<signal-details>` y `awswaf:managed:aws:bot-control:targeted:signal:<signal-details>` : se utilizan para proporcionar información adicional sobre la solicitud en algunas situaciones.

  Los siguientes son ejemplos de etiquetas de señal. No es una lista exhaustiva:

  - `awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension`: Indica la detección de una extensión del navegador que ayuda con la automatización, como Selenium IDE.

    Esta etiqueta se agrega cada vez que un usuario tiene este tipo de extensión instalada, incluso si no la está utilizando activamente. Si implementa una regla de coincidencia de etiquetas para ello, tenga en cuenta la posibilidad de que se produzcan falsos positivos en la lógica de la regla y en la configuración de las acciones. Por ejemplo, puede utilizar una acción CAPTCHA en lugar de Block, o puede combinarla con otras coincidencias de etiquetas para aumentar su confianza de que se está utilizando la automatización.
  - `awswaf:managed:aws:bot-control:signal:automated_browser`: indica que la solicitud contiene indicadores de que el navegador del cliente podría estar automatizado.

- `awswaf:managed:aws:bot-control:targeted:signal:automated_browser`— Indica que el AWS WAF token de la solicitud contiene indicadores de que el navegador del cliente podría estar automatizado.

Puede recuperar todas las etiquetas de un grupo de reglas a través de la API llamando al `DescribeManagedRuleGroup`. Las etiquetas aparecen en la propiedad `AvailableLabels` de la respuesta.

El grupo de reglas administrado de control de bots aplica etiquetas a un conjunto de bots verificables que suelen estar permitidos. El grupo de reglas no bloquea estos bots verificados. Si lo desea, puede bloquearlos o bloquear un subconjunto de ellos escribiendo una regla personalizada que utilice las etiquetas aplicadas por el grupo de reglas administrado de control de bots. Para obtener más información acerca de esto y ver ejemplos, consulte AWS WAF Control de bots.

Listado de reglas de control de bots

En esta sección se enumeran las reglas de control de bots.

> **Note**
>
> La información que publicamos sobre las reglas en los grupos de reglas de reglas AWS administradas tiene por objeto proporcionarle información suficiente para utilizarlas, pero no proporciona información que los delincuentes puedan utilizar para eludirlas. Si necesita más información de la que se encuentra en esta documentación, póngase en contacto con el centro de AWS Support.

Nombre de la regla	Descripción
`CategoryAdvertising`	Inspecciona los bots que se utilizan con fines publicitarios. Por ejemplo, puede utilizar servicios de publicidad de terceros que necesiten acceder a su sitio web mediante programación. Acción de regla; se aplica solo a los bots no verificados: Block

Nombre de la regla	Descripción
	Etiqueta: `awswaf:managed:aws:bot-control:bot:category:advertising` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .
`CategoryArchiver`	Inspecciona los bots que se utilizan con fines de archivo. Estos bots rastrean la web y capturan contenido con el fin de crear archivos. Acción de regla; se aplica solo a los bots no verificados: Block Etiqueta: `awswaf:managed:aws:bot-control:bot:category:archiver` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .

Nombre de la regla	Descripción
`CategoryContentFetcher`	Comprueba si hay bots que visiten el sitio web de la aplicación en nombre de un usuario, para buscar contenido, como fuentes RSS, o para verificar o validar su contenido. Acción de regla; se aplica solo a los bots no verificados: Block Etiqueta: `awswaf:managed:aws:bot-control:bot:category:content_fetcher` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .

Nombre de la regla	Descripción
`CategoryEmailClient`	Comprueba si hay bots que verifiquen los enlaces de los correos electrónicos que llevan al sitio web de la aplicación. Esto puede incluir bots gestionados por empresas y proveedores de correo electrónico para verificar los enlaces de los correos electrónicos y detectar los correos sospechosos. Acción de regla; se aplica solo a los bots no verificados: Block Etiqueta: `awswaf:managed:aws:bot-control:bot:category:email_client` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .

Nombre de la regla	Descripción
`CategoryHttpLibrary`	Inspecciona las solicitudes generadas por los bots desde las bibliotecas HTTP de varios lenguajes de programación. Estas pueden incluir solicitudes de API que decidas permitir o supervisar. Acción de regla; se aplica solo a los bots no verificados: Block Etiqueta: `awswaf:managed:aws:bot-control:bot:category:http_library` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .
`CategoryLinkChecker`	Inspecciona los bots que comprueban si hay enlaces rotos. Acción de regla; se aplica solo a los bots no verificados: Block Etiqueta: `awswaf:managed:aws:bot-control:bot:category:link_checker` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .

Nombre de la regla	Descripción
`CategoryMiscellaneous`	Inspecciona varios bots que no coinciden con otras categorías. Acción de regla; se aplica solo a los bots no verificados: Block Etiqueta: `awswaf:managed:aws:bot-control:bot:category:miscellaneous` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .
`CategoryMonitoring`	Inspecciona los bots que se utilizan con fines de monitorización. Por ejemplo, puede usar servicios de monitorización de bots que hagan ping periódicamente al sitio web de su aplicación para monitorizar aspectos como el rendimiento y el tiempo de actividad. Acción de regla; se aplica solo a los bots no verificados: Block Etiqueta: `awswaf:managed:aws:bot-control:bot:category:monitoring` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .

Nombre de la regla	Descripción
`CategoryScrapingFramework`	Inspecciona los bots en los sistemas de rastreo web, que se utilizan para automatizar el rastreo y la extracción de contenido de los sitios web. Acción de regla; se aplica solo a los bots no verificados: Block Etiqueta: `awswaf:managed:aws:bot-control:bot:category:scraping_framework` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .
`CategorySearchEngine`	Inspecciona los bots de los motores de búsqueda, que rastrean los sitios web para indexar el contenido y hacer que la información esté disponible para los resultados de los motores de búsqueda. Acción de regla; se aplica solo a los bots no verificados: Block Etiqueta: `awswaf:managed:aws:bot-control:bot:category:search_engine` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .

Nombre de la regla	Descripción
`CategorySecurity`	Inspecciona los bots que escanean las aplicaciones web en busca de vulnerabilidades o que realizan auditorías de seguridad. Por ejemplo, puede utilizar un proveedor de seguridad externo que escanee, monitoree o audite la seguridad de su aplicación web. Acción de regla; se aplica solo a los bots no verificados: Block Etiqueta: `awswaf:managed:aws:bot-control:bot:category:security` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .

Nombre de la regla	Descripción
`CategorySeo`	Inspecciona los bots que se utilizan para la optimización de motores de búsqueda. Por ejemplo, puede usar herramientas de motores de búsqueda que rastreen su sitio para ayudarle a mejorar su posicionamiento entre los motores de búsqueda. Acción de regla; se aplica solo a los bots no verificados: Block Etiqueta: `awswaf:managed:aws:bot-control:bot:category:seo` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .

Nombre de la regla	Descripción
`CategorySocialMedia`	Inspecciona los bots que utilizan las plataform as de redes sociales para proporcionar resúmenes de contenido cuando los usuarios comparten su contenido. Acción de regla; se aplica solo a los bots no verificados: Block Etiqueta: `awswaf:managed:aws:bot-control:bot:category:social_media` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .
`CategoryAI`	Inspecciona los bots de inteligencia artificial (IA). Acción de la regla: Block Etiqueta: `awswaf:managed:aws:bot-control:bot:category:ai`

Nombre de la regla	Descripción
`SignalAutomatedBrowser`	Inspecciona la solicitud en busca de indicadores de que el navegador del cliente podría estar automatizado. Se pueden usar navegadores automatizados para probar o rastrear. Por ejemplo, puede utilizar estos tipos de navegadores para monitorizar o verificar el sitio web de su aplicación. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:bot-control:signal:automated_browser`
`SignalKnownBotDataCenter`	Inspecciona los indicadores de los centros de datos que suelen utilizar los bots. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:bot-control:signal:known_bot_data_center`
`SignalNonBrowserUserAgent`	Inspecciona las cadenas de los agentes de usuario que no parecen provenir de un navegador web. Esta categoría puede incluir solicitudes API. Acción de la regla: Block Etiqueta: `awswaf:managed:aws:bot-control:signal:non_browser_user_agent`

Nombre de la regla	Descripción
`TGT_VolumetricIpTokenAbsent`	Inspecciona 5 o más solicitudes de un cliente en los últimos 5 minutos que no incluyan un token de desafío válido. Para obtener informaci ón acerca de los tokens, consulte AWS WAF tokens de solicitud web. **Note** Es posible que esta regla coincida en una solicitud que tiene un token si a las solicitudes del mismo cliente les han faltado tokens recientemente. El umbral al que se aplica esta regla puede variar ligeramente debido a la latencia. Esta regla gestiona los tokens faltantes de manera diferente al etiquetado de los tokens: `awswaf:managed:token:absent` . El etiquetado de los tokens etiqueta las solicitudes individuales que no tienen un token. Esta regla mantiene un recuento de las solicitudes a las que les falta su token para cada IP de cliente y las compara con los clientes que superan el límite. Acción de regla, que se aplica solo a los clientes que no son bots verificados: Challenge Etiqueta: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:ip:token_absent` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el

Nombre de la regla	Descripción
	etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .

Nombre de la regla	Descripción
`TGT_VolumetricSession`	Inspecciona un número anormalmente alto de solicitudes de una sesión de cliente en un período de 5 minutos. La evaluación se basa en una comparación con las líneas base volumétricas estándar y se basa en patrones de AWS WAF tráfico históricos. Esta inspección solamente se aplica cuando la solicitud web tiene un token. Los tokens se agregan a las solicitudes por los SDK de integración de y por las acciones de regla CAPTCHA y Challenge. Para obtener más información, consulte AWS WAF tokens de solicitud web. **Note** Esta regla puede tardar 5 minutos en entrar en vigor después de activarla. Bot Control identifica el comportamiento anómalo del tráfico web comparando el tráfico actual con las líneas base de tráfico que calcula. AWS WAF Acción de regla, que se aplica solo a los clientes que no son bots verificados: CAPTCHA Etiqueta: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:high`

Nombre de la regla	Descripción
	El grupo de reglas aplica las siguientes etiquetas a las solicitudes de volumen medio y bajo que superan un umbral mínimo. Para estos niveles, la regla no realiza ninguna acción, independientemente de si el cliente está verificado: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:medium` y `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:low` . En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .

Nombre de la regla	Descripción
`TGT_SignalAutomatedBrowser`	Inspecciona el token de la solicitud en busca de indicadores que el navegador del cliente podría estar automatizado. Para obtener más información, consulte AWS WAF caracterí sticas del token. Esta inspección solamente se aplica cuando la solicitud web tiene un token. Los tokens se agregan a las solicitudes por los SDK de integración de y por las acciones de regla CAPTCHA y Challenge. Para obtener más información, consulte AWS WAF tokens de solicitud web. Acción de regla, que se aplica solo a los clientes que no son bots verificados: CAPTCHA Etiqueta: `awswaf:managed:aws:bot-control:targeted:signal:automated_browser` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .

Nombre de la regla	Descripción
`TGT_SignalBrowserInconsistency`	Inspecciona si los datos de interrogación del navegador son inconsistentes. Para obtener más información, consulte AWS WAF caracterí sticas del token. Esta inspección solamente se aplica cuando la solicitud web tiene un token. Los tokens se agregan a las solicitudes por los SDK de integración de y por las acciones de regla CAPTCHA y Challenge. Para obtener más información, consulte AWS WAF tokens de solicitud web. Acción de regla, que se aplica solo a los clientes que no son bots verificados: CAPTCHA Etiqueta: `awswaf:managed:aws:bot-control:targeted:signal:browser_inconsistency` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` .

Nombre de la regla	Descripción
`TGT_TokenReuseIp`	Inspecciona el uso de un único token entre más de 5 direcciones IP distintas. **Note** Los umbrales a los que se aplica esta regla pueden variar ligeramente debido a la latencia. Es posible que algunas solicitudes superen el límite antes de que se aplique la acción de la regla. Acción de la regla: Count Etiqueta: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:token_reuse:ip`

Nombre de la regla	Descripción
`TGT_ML_CoordinatedActivityMedium` y `TGT_ML_CoordinatedActivityHigh`	Inspecciona si hay algún comportamiento anómalo coherente con la actividad distribuida y coordinada de los bots. Los niveles de las reglas indican el nivel de confianza de que un grupo de solicitudes participen en un ataque coordinado. **Note** Estas reglas solamente se ejecutan si el grupo de reglas está configurado para usar el machine learning (ML). Para obtener información acerca de cómo configurar esta opción, consulte Añadir el grupo de reglas gestionado por AWS WAF Bot Control a su ACL web. AWS WAF realiza esta inspección mediante un análisis de aprendizaje automático de las estadísticas de tráfico del sitio web. AWS WAF analiza el tráfico web cada pocos minutos y optimiza el análisis para detectar bots de baja intensidad y larga duración que se distribuyen en muchas direcciones IP. Es posible que estas reglas coincidan en un número muy reducido de solicitudes antes de determinar que no se está produciendo un ataque coordinado. Por lo tanto, si solo ve una o dos coincidencias, los resultados podrían ser falsos positivos. Sin embargo, si ve muchas

Nombre de la regla	Descripción
	coincidencias de estas reglas, es probable que esté siendo víctima de un ataque coordinado. **Note** Estas reglas pueden tardar hasta 24 horas en entrar en vigor si activa las reglas específicas del control de bots con la opción de ML. Bot Control identifica el comportamiento anómalo del tráfico web comparando el tráfico actual con las líneas base de tráfico calculadas. AWS WAF AWS WAF Solo calcula las líneas de base cuando utilizas las reglas específicas de Bot Control con la opción de aprendizaje automático, y establecer líneas de base significativas puede llevar hasta 24 horas. Actualizamos periódicamente nuestros modelos de aprendizaje automático para adaptarlos a estas reglas, a fin de mejorar las predicciones de los bots. Si observas un cambio repentino y sustancial en las prediccio nes de los bots que contienen estas reglas, ponte en contacto con tu administrador de cuentas o abre un caso en AWS Support Center. Acciones de regla, que se aplican solamente a los clientes que no son bots verificados: • Media: Count

Nombre de la regla	Descripción
	• Alta: Count Etiquetas: `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:medium` y `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:high` En el caso de los bots verificados, el grupo de reglas no realiza ninguna acción, pero añade el etiquetado de la regla y la etiqueta `awswaf:managed:aws:bot-control:bot:verified` . El grupo de reglas también agrega la etiqueta `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low` para indicar un nivel de confianza bajo, pero no aplica ninguna regla ni realiza ninguna acción en relación con estas solicitudes.

Implementaciones para grupos de reglas de reglas AWS administradas versionados

AWS implementa los cambios en sus grupos de reglas de AWS Managed Rules versionados en tres implementaciones estándar: release candidate, versión estática y versión predeterminada. Además, a veces es AWS posible que necesite lanzar una implementación de excepción o revertir una implementación de versión predeterminada.

> **Note**
>
> Esta sección solo se aplica a los grupos de reglas de AWS Managed Rules que están versionados. El único grupo de reglas que no está versionado es el grupo de reglas de reputación IP.

Temas

Notificaciones para despliegues de grupos de reglas de AWS Managed Rules

Todos los grupos de reglas de AWS Managed Rules versionados proporcionan notificaciones de actualización de SNS para las implementaciones y todos usan el mismo tema de SNS: Amazon Resource Name (ARN). El único grupo de reglas que no está versionado es el grupo de reglas de reputación IP.

En el caso de las implementaciones que afectan a sus protecciones, como los cambios en la versión predeterminada, AWS proporciona notificaciones de SNS para informarle sobre las implementaciones planificadas y para avisarle de cuándo se está iniciando una implementación. En el caso de las implementaciones que no afectan a sus protecciones, como las de versión candidata y estática, es posible que AWS le notifique una vez que la implementación haya comenzado o incluso una vez finalizada. Al finalizar la implementación de una nueva versión estática, AWS actualiza esta guía en el registro de cambios AWS Registro de cambios de reglas administradas y en la página del historial del documento en. Historial de documentos

Para recibir todas las actualizaciones relacionadas con AWS los grupos de reglas de reglas AWS administradas, suscríbase a la fuente RSS desde cualquier página HTML de esta guía y suscríbase al tema de SNS relativo a los grupos de reglas de reglas AWS administradas. Para obtener

información sobre la suscripción a las notificaciones de SNS, consulte. Recepción de notificaciones sobre nuevas versiones y actualizaciones de un grupo de reglas administrado

Contenido de las notificaciones de SNS

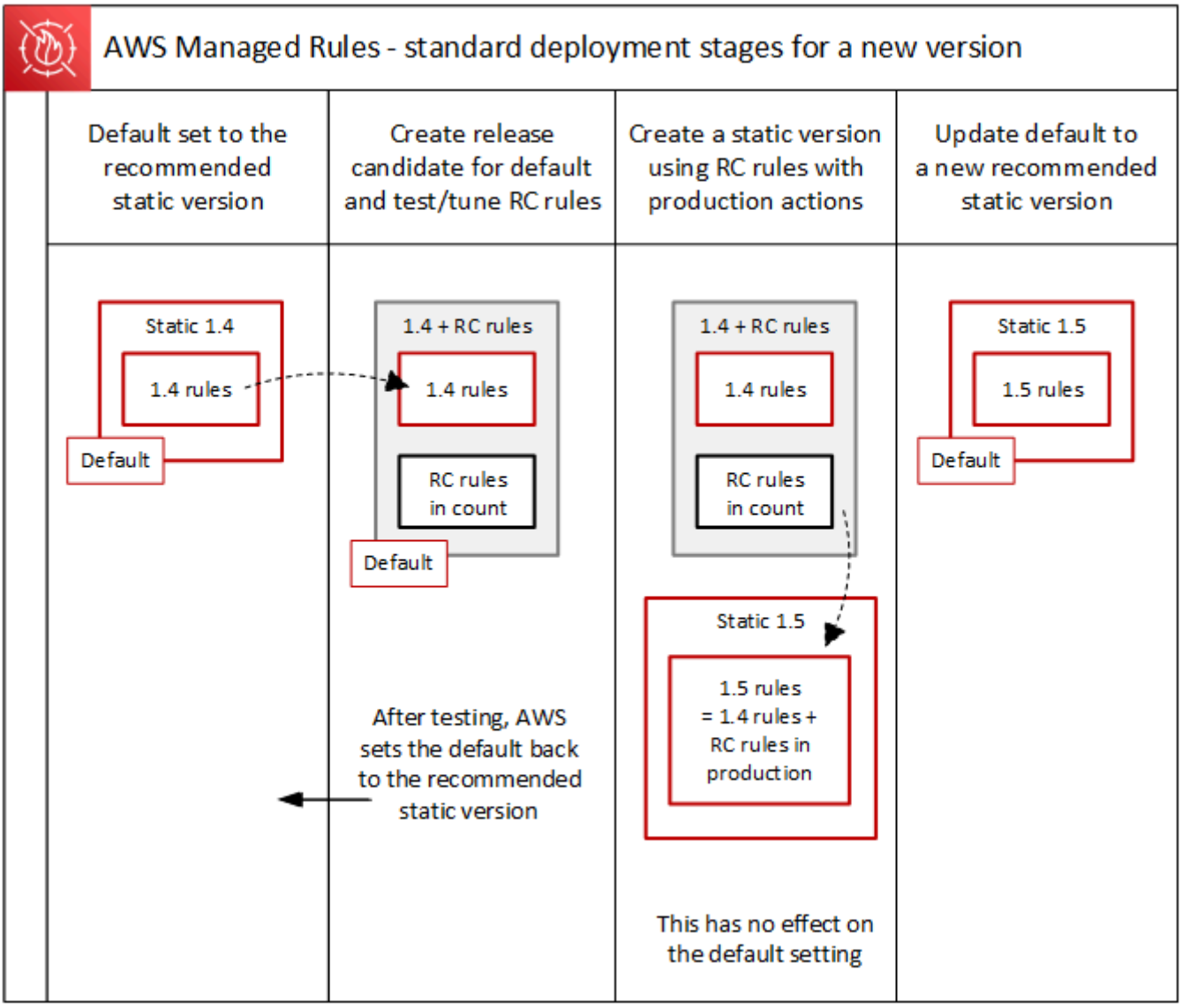
Los campos de las notificaciones de Amazon SNS siempre incluyen el asunto, el mensaje y. MessageAttributes Los campos adicionales dependen del tipo de mensaje y del grupo de reglas administrado al que se destine la notificación. A continuación, se muestra un ejemplo de lista de notificaciones para `AWSManagedRulesCommonRuleSet`.

```
{
    "Type": "Notification",
    "MessageId": "4286b830-a463-5e61-bd15-e1ae72303868",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:MyTopic",
    "Subject": "New version available for rule group AWSManagedRulesCommonRuleSet",
    "Message": "Welcome to AWSManagedRulesCommonRuleSet version 1.5! We've updated
 the regex specification in this version to improve protection coverage, adding
 protections against insecure deserialization. For details about this change, see
 http://updatedPublicDocs.html. Look for more exciting updates in the future! ",
    "Timestamp": "2021-08-24T11:12:19.810Z",
    "SignatureVersion": "1",
    "Signature": "EXAMPLEHXgJm...",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
f3ecfb7224c7233fe7bb5f59f96de52f.pem",
    "SubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=ConfirmSubscription&TopicArn=arn:aws:sns:us-
west-2:123456789012:MyTopic&Token=2336412f37...",
    "MessageAttributes": {
        "major_version": {
            "Type": "String",
            "Value": "v1"
        },
        "managed_rule_group": {
            "Type": "String",
            "Value": "AWSManagedRulesCommonRuleSet"
        }
    }
}
```

Descripción general de las implementaciones estándar de las reglas AWS administradas

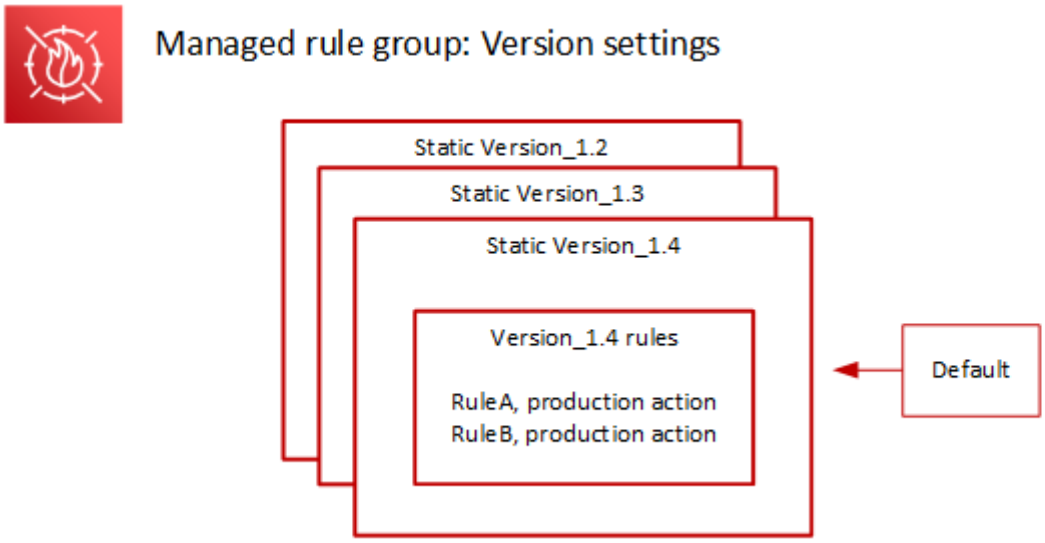
AWS implementa la nueva funcionalidad de reglas AWS administradas mediante tres etapas de implementación estándar: versión candidata, versión estática y versión predeterminada.

En el siguiente diagrama, se muestran estas implementaciones estándar. Cada uno de estos se describe con mayor detalle en las secciones siguientes.



Estados de versión típicos de las reglas AWS administradas

Normalmente, un grupo de reglas gestionado versionado tiene varias versiones estáticas que no han caducado y la versión predeterminada apunta a la versión estática recomendada. AWS En la siguiente imagen, se muestra un ejemplo del conjunto típico de versiones estáticas y de la configuración de la versión predeterminada.



La acción de producción para la mayoría de las reglas en una versión estática es Block, pero puede estar configurada en algo diferente. Para obtener información detallada sobre la configuración de las acciones de reglas, consulte la lista de reglas de cada grupo de reglas en AWS Lista de grupos de reglas de Managed Rules.

Publicar las implementaciones candidatas para AWS Managed Rules

Cuando AWS un conjunto de reglas candidato cambia para un grupo de reglas gestionado, los pone a prueba en una implementación candidata de versión temporal. AWS evalúa las reglas candidatas en el modo de recuento comparándolas con el tráfico de producción y realiza las últimas actividades de ajuste, incluida la mitigación de los falsos positivos. AWS Las pruebas publican las reglas candidatas de esta forma para todos los clientes que utilizan la versión predeterminada del grupo de reglas. Las implementaciones de la versión candidata a ser lanzada no se aplican a los clientes que usan una versión estática del grupo de reglas.

Si utiliza la versión predeterminada, una implementación de la versión candidata a ser lanzada no alterará la forma en que el grupo de reglas administra su tráfico web. Es posible que observe lo siguiente mientras se prueban las reglas candidatas:

- El nombre de la versión predeterminada cambia de `Default (using Version_X.Y)` a `Default (using Version_X.Y_PLUS_RC_COUNT)`.
- Métricas de recuento adicionales en Amazon CloudWatch con `RC_COUNT` sus nombres. Estas se generan mediante las reglas candidatas a ser lanzadas.

AWS prueba una versión candidata durante aproximadamente una semana, luego la elimina y restablece la versión predeterminada a la versión estática recomendada actualmente.

AWS lleva a cabo los siguientes pasos para la implementación de una versión candidata:

1. Crear la versión candidata: AWS añade una versión candidata en función de la versión estática recomendada actualmente, que es la versión a la que apunta la versión predeterminada.

   El nombre de la versión candidata a ser lanzada es el nombre de la versión estática al que se añade `_PLUS_RC_COUNT`. Por ejemplo, si la versión estática actualmente recomendada es `Version_2.1`, la versión candidata a ser lanzada recibirá el nombre `Version_2.1_PLUS_RC_COUNT`.

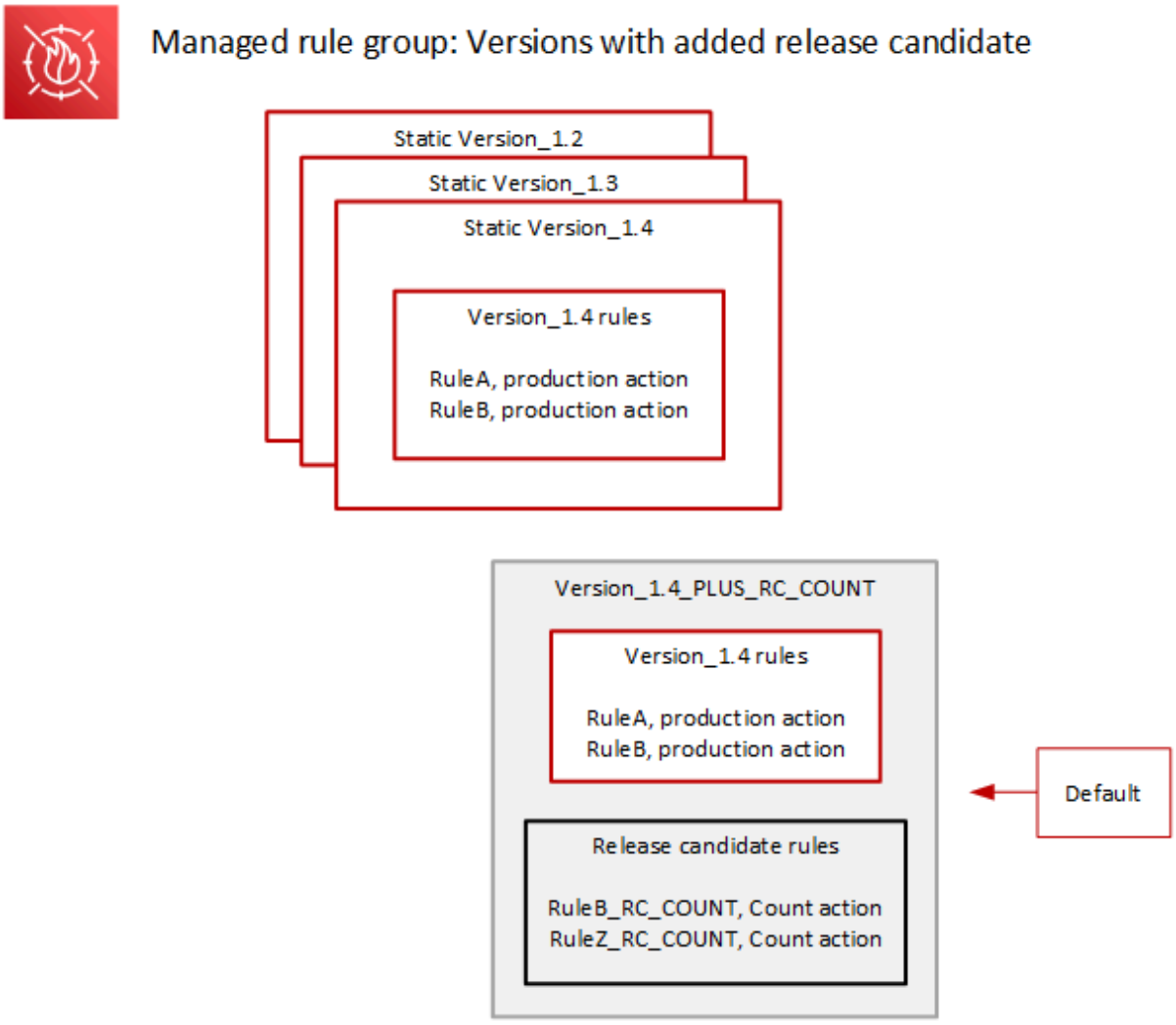
   La versión candidata a ser lanzada contiene las siguientes reglas:

   - Las reglas se copiaron exactamente de la versión estática recomendada actualmente, sin cambios en la configuración de las reglas.
   - Reglas candidatas nuevas con la acción de regla configurada en Count y cuyos nombres terminen en `_RC_COUNT`.

     La mayoría de las reglas de las versiones candidatas incluyen propuestas de mejora para las reglas que ya existen en el grupo de reglas. El nombre de cada una de estas reglas es el nombre de la regla existente al que se añade `_RC_COUNT`.
2. Defina la versión predeterminada como la versión candidata y pruébela: AWS configura la versión predeterminada para que apunte a la nueva versión candidata, a fin de realizar pruebas comparándolas con el tráfico de producción. Las pruebas suelen tardar alrededor de una semana.

   Verá que el nombre de la versión predeterminada cambia de una versión que solo indica la versión estática, por ejemplo `Default (using Version_1.4)`, a una que indica la versión estática más las reglas de la versión candidata a ser lanzada, por ejemplo `Default (using Version_1.4_PLUS_RC_COUNT)`. Este esquema de nomenclatura le permite identificar qué versión estática utiliza para gestionar el tráfico web.

   El siguiente diagrama muestra el estado de las versiones del grupo de reglas de ejemplo en este momento.



Las reglas candidatas a ser lanzadas siempre se configuran con una acción Count, por lo que no alteran la forma en que el grupo de reglas administra el tráfico web.

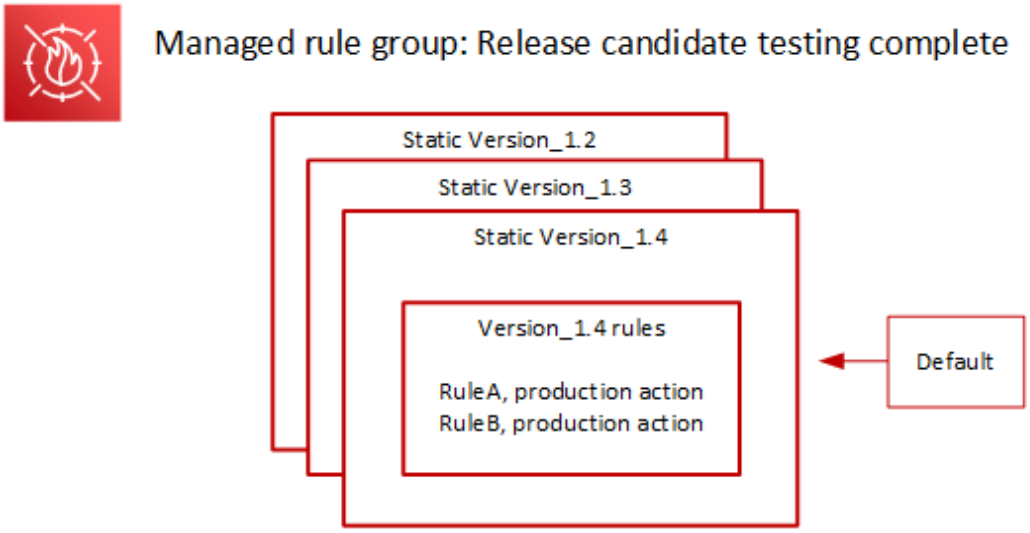
Las reglas de release candidate generan métricas de CloudWatch recuento de Amazon que se AWS utilizan para verificar el comportamiento e identificar los falsos positivos. AWS realiza los ajustes necesarios para ajustar el comportamiento de las reglas de recuento de candidatos a publicación.

La versión candidata a ser lanzada no es estática y no puede seleccionarla de la lista de versiones de grupos de reglas estáticas. Solamente puede ver el nombre de la versión candidata a ser lanzada en la especificación de la versión predeterminada.

3. Devuelve la versión predeterminada a la versión estática recomendada: tras probar las reglas de la versión candidata, AWS vuelve a establecer la versión estática recomendada actualmente para la versión predeterminada. La configuración predeterminada del nombre de la versión elimina

la `_PLUS_RC_COUNT` terminación y el grupo de reglas deja de generar métricas de CloudWatch recuento para las reglas de la versión candidata. Se trata de un cambio silencioso y no es lo mismo que implementar una reversión de una versión predeterminada.

El siguiente diagrama muestra el estado de las versiones del grupo de reglas de ejemplo una vez finalizadas las pruebas de la candidata a ser lanzada.



Calendario y notificaciones

AWS despliega versiones candidatas según sea necesario, para probar las mejoras en un grupo de reglas.

- SNS: AWS envía una notificación de SNS al inicio de la implementación. La notificación indica el tiempo estimado durante el que se probará la versión candidata. Una vez finalizadas las pruebas, devuelve AWS silenciosamente la configuración predeterminada de la versión estática, sin necesidad de una segunda notificación.
- Registro de cambios: AWS no actualiza el registro de cambios ni otras partes de esta guía para este tipo de implementación.

Implementaciones de versiones estáticas para reglas AWS administradas

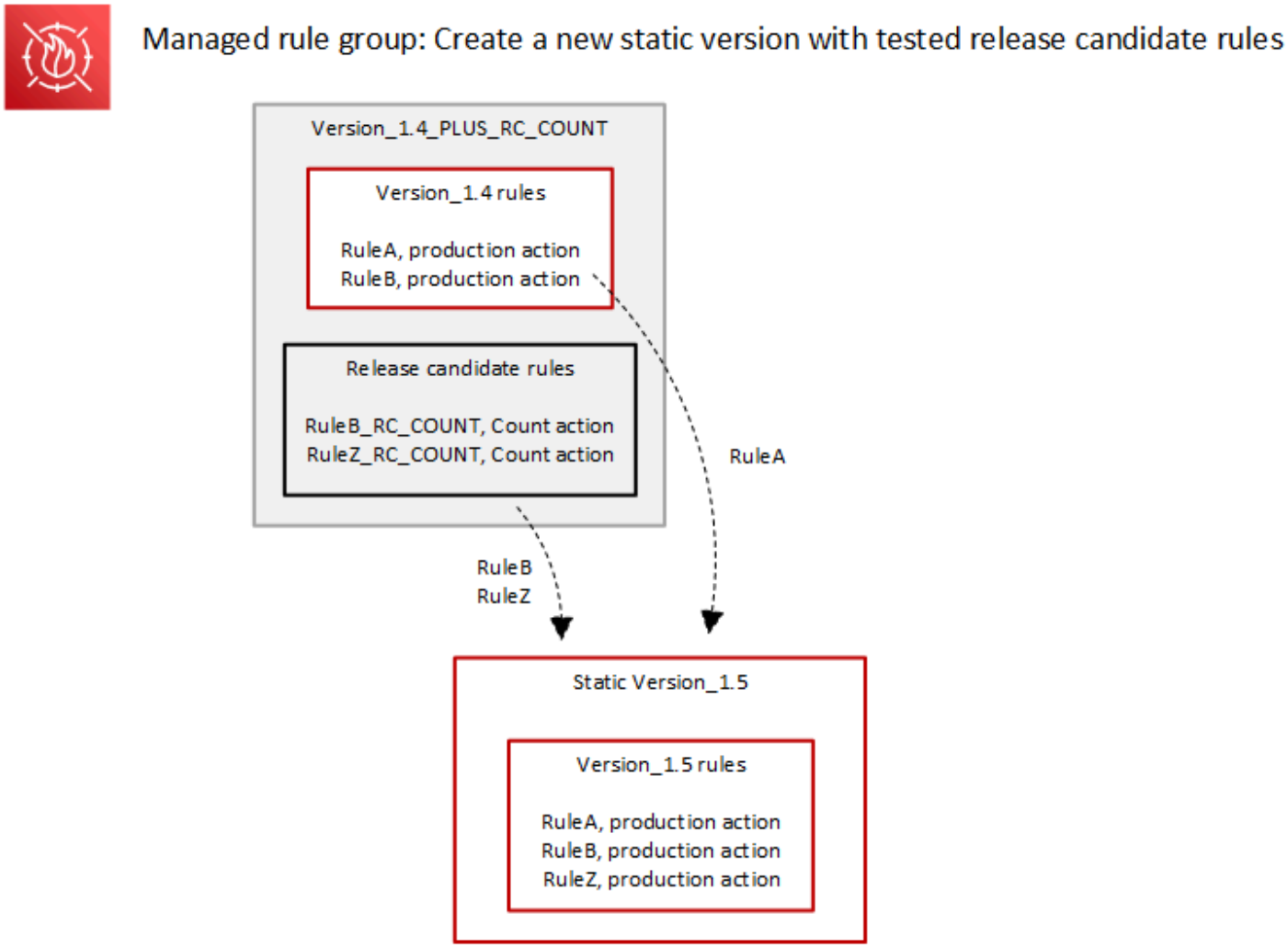
Cuando AWS determina que una versión candidata proporciona cambios valiosos al grupo de reglas, AWS implementa una nueva versión estática para el grupo de reglas basada en la versión candidata. Esta implementación no cambia la versión predeterminada del grupo de reglas.

La nueva versión estática contiene las siguientes reglas para la versión candidata:

- Reglas de la versión estática anterior que no tienen un candidato de reemplazo entre las reglas de la candidata a ser lanzada.
- Reglas candidatas a ser lanzadas con los cambios siguientes:
  - AWS cambia el nombre de la regla eliminando el sufijo `_RC_COUNT` Release Candidate.
  - AWS cambia las acciones de la regla Count a sus acciones de la regla de producción.

  En el caso de las reglas candidatas a ser lanzadas que sustituyan a reglas anteriores existentes, se sustituirá la funcionalidad de las reglas anteriores de la nueva versión estática.

El siguiente diagrama muestra la creación de la nueva versión estática a partir de la candidata a ser lanzada.



Tras la implementación, la nueva versión estática está disponible para que la pruebe y la utilice en sus protecciones si así lo desea. Puede revisar las acciones y descripciones de las reglas nuevas

y actualizadas en las listas de reglas del grupo de reglas en AWS Lista de grupos de reglas de Managed Rules.

Una versión estática es inmutable tras el despliegue y solo cambia cuando AWS caduca. Para obtener información sobre el ciclo de vida de las versiones, consulte Grupos de reglas gestionados versionados.

Calendario y notificaciones

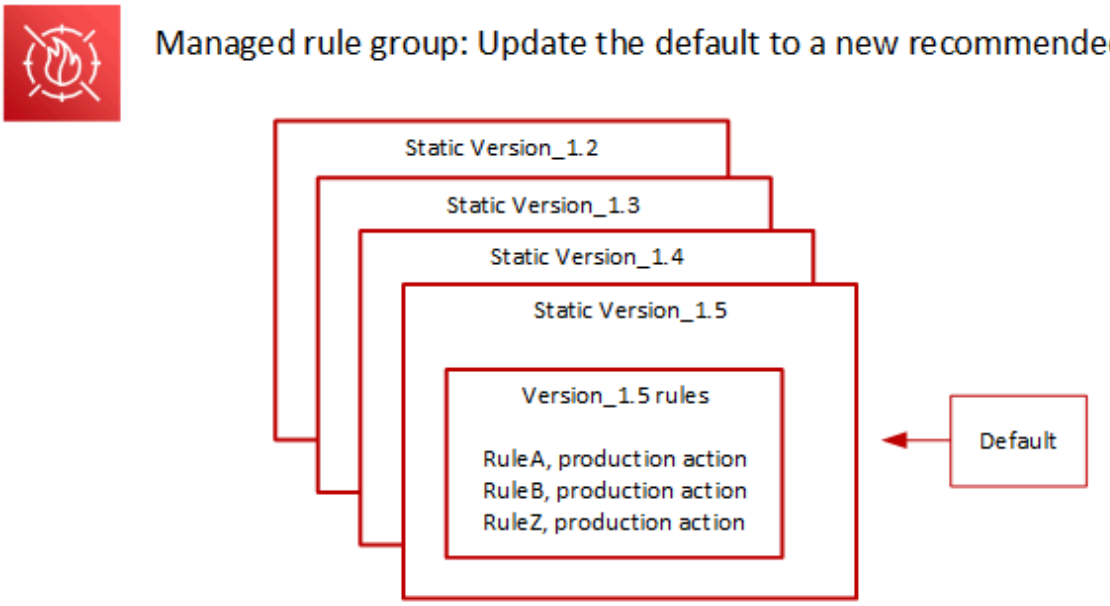
AWS implementa una nueva versión estática según sea necesario para implementar mejoras en la funcionalidad de los grupos de reglas. La implementación de una versión estática no afecta a la configuración de la versión predeterminada.

- SNS: AWS envía una notificación de SNS cuando se completa la implementación.
- Registro de cambios: una vez completada la implementación en todos los lugares disponibles, AWS actualiza la definición del grupo de reglas de esta guía según sea necesario y, a continuación, anuncia la publicación en el registro de cambios del grupo de reglas de reglas AWS administradas y en la página del historial de la documentación. AWS WAF

Implementaciones de versiones predeterminadas para AWS Managed Rules

Cuando AWS determina que una nueva versión estática proporciona una protección mejorada para el grupo de reglas en comparación con la versión predeterminada actual, AWS actualiza la versión predeterminada a la nueva versión estática. AWS podría publicar varias versiones estáticas antes de convertir una de ellas en la versión predeterminada del grupo de reglas.

El siguiente diagrama muestra el estado de las versiones del grupo de reglas de ejemplo después de AWS mover la configuración de la versión predeterminada a la nueva versión estática.



Antes de implementar este cambio en la versión predeterminada, AWS proporciona notificaciones para que pueda probar los próximos cambios y prepararse para ellos. Si utiliza la versión predeterminada, no podrá realizar ninguna acción y permanecer en ella durante la actualización. Si, por el contrario, desea retrasar el cambio a la nueva versión, antes del inicio planificado de la implementación de la versión predeterminada, puede configurar explícitamente su grupo de reglas para que utilice la versión estática establecida de forma predeterminada.

Calendario y notificaciones

AWS actualiza la versión predeterminada cuando recomienda una versión estática diferente para el grupo de reglas que la que se está utilizando actualmente.

- SNS: AWS envía una notificación de SNS al menos una semana antes del día de implementación previsto y, después, otra el día de la implementación, al inicio de la implementación. Cada notificación incluye el nombre del grupo de reglas, la versión estática a la que se actualiza la versión predeterminada, la fecha de despliegue y el momento programado del despliegue para cada AWS región en la que se realiza la actualización.
- Registro de cambios: AWS no actualiza el registro de cambios ni otras partes de esta guía para este tipo de implementación.

Implementaciones de excepciones para las reglas administradas de AWS

AWS podría omitir las etapas de implementación estándar para implementar rápidamente actualizaciones que aborden los riesgos de seguridad críticos. Una implementación excepcional puede incluir cualquiera de los tipos de implementación estándar y puede implementarse rápidamente en todas las AWS regiones.

AWS proporciona una notificación con la mayor antelación posible para las implementaciones de excepciones.

Calendario y notificaciones

AWS realiza despliegues de excepciones solo cuando es necesario.

- SNS: AWS envía una notificación de SNS con la mayor antelación posible al día de despliegue previsto y, a continuación, otra al inicio del despliegue. Cada notificación incluye el nombre del grupo de reglas, el cambio que se está realizando y la fecha de implementación.
- Registro de cambios: si la implementación es para una versión estática, una vez completada la implementación en todos los lugares disponibles, AWS actualiza la definición del grupo de reglas de esta guía según sea necesario y, a continuación, anuncia la versión en el registro de cambios del grupo de reglas de reglas AWS administradas y en la página del historial de la documentación. AWS WAF

Reversiones de implementación predeterminadas para las reglas AWS administradas

En determinadas condiciones, AWS podría revertir la versión predeterminada a su configuración anterior. La reversión suele tardar menos de diez minutos en todas las AWS regiones.

AWS realiza una reversión solo para mitigar un problema importante en una versión estática, como un nivel inaceptablemente alto de falsos positivos.

Tras revertir la configuración de la versión predeterminada, AWS acelera tanto la caducidad de la versión estática que tiene el problema como el lanzamiento de una nueva versión estática para solucionar el problema.

Calendario y notificaciones

AWS revierte las versiones predeterminadas solo cuando es necesario.

- SNS: AWS envía una única notificación de SNS en el momento de la reversión. La notificación incluye el nombre del grupo de reglas, la versión en la que se está configurando la versión

predeterminada y la fecha de implementación. Este tipo de implementación es muy rápido, por lo que la notificación no proporciona información sobre los plazos de las regiones.

- Registro de cambios: AWS no actualiza el registro de cambios ni otras partes de esta guía para este tipo de implementación.

AWS Descargo de responsabilidad de Managed Rules

AWS Las reglas administradas están diseñadas para protegerlo de las amenazas web más comunes. Cuando se utilizan de acuerdo con la documentación, los grupos de reglas de reglas AWS administradas añaden otro nivel de seguridad a sus aplicaciones. Sin embargo, los grupos de reglas de reglas AWS administradas no pretenden sustituir sus responsabilidades de seguridad, que vienen determinadas por los AWS recursos que seleccione. Consulte el modelo de responsabilidad compartida para asegurarse de que sus recursos AWS estén debidamente protegidos.

AWS Registro de cambios de reglas administradas

En esta sección, se enumeran los cambios en las reglas AWS administradas AWS WAF desde su publicación en noviembre de 2019.

> **Note**
>
> Este registro de cambios informa de los cambios en las reglas y los grupos de reglas de AWS Managed Rules for. AWS WAF
> En el caso deGrupos de reglas de reputación de IP, este registro de cambios informa de los cambios en las reglas y el grupo de reglas, así como de los cambios significativos en las fuentes de las listas de direcciones IP que utilizan las reglas. No informa de los cambios en las propias listas de direcciones IP, debido a la naturaleza dinámica de esas listas. Si tiene preguntas sobre las listas de direcciones IP, póngase en contacto con su administrador de cuentas o abra un caso en AWS Support Center.

Reglas y grupos de reglas	Descripción	Fecha
AWS WAF Grupo de reglas de control de bots AWS WAF Grupo de reglas de prevención de apropiación de	Los grupos de reglas de bots y fraudes ahora están versionados. Si utilizas alguno de estos grupos de reglas,	29 de mayo de 2020

Reglas y grupos de reglas	Descripción	Fecha
cuentas (ATP) para el control del fraude AWS WAF Grupo de reglas de prevención del fraude (ACFP) para la creación de cuentas de Control de Fraude	esta actualización no cambia la forma en que gestionan el tráfico web. Esta actualización establece la versión actual del grupo de reglas en la versión estática 1.0 y establece la versión predeterminada para que apunte a ella. Para obtener más informaci ón sobre las reglas administr adas versionadas, consulte lo siguiente: • Grupos de reglas gestionad os versionados • Implementaciones para grupos de reglas de reglas AWS administradas versionados • Recepción de notificaciones sobre nuevas versiones y actualizaciones de un grupo de reglas administrado	

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado para el sistema operativo POSIX • UNIXShellCommandsVariables_QUERYARGUMENTS • UNIXShellCommandsVariables_QUERYSTRING • UNIXShellCommandsVariables_HEADER • UNIXShellCommandsVariables_BODY	Se publicó la versión estática 3.0 de este grupo de reglas. Esto no cambia la configuración de la versión predeterminada. Se quitó UNIXShellCommandsVariables_QUERYARGUMENTS y se sustituyó por UNIXShellCommandsVariables_QUERYSTRING. Si tiene reglas que coinciden en la etiqueta UNIXShellCommandsVariables_QUERYARGUMENTS, cuando utilice esta versión, cámbielas para que coincidan con las de la etiqueta UNIXShellCommandsVariables_QUERYSTRING. La nueva etiqueta es awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString. Se agregó la regla UNIXShellCommandsVariables_HEADER, que coincide con todos los encabezados. Se actualizaron todas las reglas del grupo de reglas	28-05-2022

Reglas y grupos de reglas	Descripción	Fecha
	administrado con una lógica de detección mejorada. Se corrigió el uso documentado de mayúsculas en la etiqueta para`UNIXShellCommandsVariables_BODY` .	
Grupo de reglas administrado del conjunto de reglas básicas (CRS) • `CrossSiteScripting*`	Publicada la versión estática 1.12 de este grupo de reglas. Se agregaron firmas a todas las reglas de scripts entre sitios para mejorar la detección y reducir los falsos positivos.	21-05-2022
Grupo de reglas administrado de la base de datos SQL • `SQLi_BODY` • `SQLi_QUERYARGUMENTS` • `SQLiExtendedPatterns_QUERYARGUMENTS`	Publicada la versión estática 1.2 de este grupo de reglas. Se agregó la transformación de `JS_DECODE` texto a las reglas enumeradas.	14 de mayo de 2022

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado de entradas incorrectas conocidas • JavaDeserializationRCE_BODY • JavaDeserializationRCE_QUERYSTRING • Log4JRCE_QUERYSTRING • Log4JRCE_BODY • Log4JRCE_HEADER	Publicada la versión estática 1.22 de este grupo de reglas. Se agregó la transformación de JS_DECODE texto a las reglas enumeradas.	2024-05-08
Grupo de reglas administrado para el sistema operativo POSIX	Se lanzó la versión estática 2.2 de este grupo de reglas. Se agregó la transformación de JS_DECODE texto a ambas reglas.	2024-05-08
Grupo de reglas administrado para el sistema operativo Windows • PowerShellCommands_BODY	Se lanzó la versión estática 2.1 de este grupo de reglas. Se agregaron firmas para mejorar la detección. PowerShellCommands_BODY	2024-05-03

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado con lista de reputación de IP de Amazon • `AWSManagedIPReputationList`	Se actualizaron las fuentes de la lista de reputación IP para mejorar la identificación de las direcciones que participan activamente en actividades maliciosas y reducir los falsos positivos. Esta actualización no incluye una nueva versión porque este grupo de reglas no está versionado.	13-03-2022
Grupo de reglas administrado de entradas incorrectas conocidas	Se lanzó la versión estática 1.21 de este grupo de reglas. Se agregaron firmas para mejorar la detección y reducir los falsos positivos.	2023-12-16

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado de entradas incorrectas conocidas • `ExploitablePaths_URIPATH`	Se lanzó la versión estática 1.20 de este grupo de reglas. Se actualizó la regla `ExploitablePaths_URIPATH` para agregar la detección de las solicitudes que coincidan con la vulnerabilidad de autorización inadecuada CVE-2023-22518 de Atlassian Confluence. Esta vulnerabilidad afecta a todas las versiones del centro de datos y del servidor de Confluence. Para obtener más información, consulte NIST: National Vulnerability Database: CVE-2023-22518 Detail.	2023-12-14
Grupo de reglas administrado del conjunto de reglas básicas (CRS) • `CrossSiteScripting*`	Se lanzó la versión estática 1.11 de este grupo de reglas. Se agregaron firmas a todas las reglas de scripts entre sitios para mejorar la detección y reducir los falsos positivos.	2023-12-06

Reglas y grupos de reglas	Descripción	Fecha
AWS WAF Grupo de reglas de control de bots • Nueva etiqueta: `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low`	Se agregó la etiqueta de actividad coordinada baja a las etiquetas de nivel de protección específicas del grupo de reglas. Esta etiqueta no está asociada a ninguna regla. Este etiquetado se suma a las reglas y etiquetas de nivel medio y alto.	2023-12-05
Etiquetas de control de bots • Etiqueta: `awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension`	Se agregó una etiqueta de señal al grupo de reglas que indica la detección de una extensión del navegador que ayuda a la automatización. Esta etiqueta no es específica de una regla individual.	14-11-2020
Grupo de reglas administrado del conjunto de reglas básicas (CRS) • `EC2MetaDataSSRF_QUERYARGUMENTS`	Se lanzó la versión estática 1.10 de este grupo de reglas. Se actualizó una regla para mejorar la detección y reducir los falsos positivos.	2023-11-02

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado del conjunto de reglas básicas (CRS) • `EC2MetaDataSSRF_BODY` • `EC2MetaDataSSRF_COOKIE` • `EC2MetaDataSSRF_URIPATH` • `EC2MetaDataSSRF_QUERYARGUMENTS`	Se lanzó la versión estática 1.9 de este grupo de reglas. Se actualizaron una regla para mejorar la detección y reducir los falsos positivos.	2023-10-30
Grupo de reglas administrado para el sistema operativo POSIX • `UNIXShellCommandsVariables_QUERYARGUMENTS`	Se lanzó la versión estática 2.1 de este grupo de reglas. Se actualizó la regla de argumentos de consulta para mejorar la detección.	2023-10-12

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado del conjunto de reglas básicas (CRS) • `GenericLFI_QUERYARGUMENTS` • `GenericLFI_URIPATH` • `RestrictedExtensions_URIPATH` • `RestrictedExtensions_QUERYARGUMENTS`	Se lanzó la versión estática 1.8 de este grupo de reglas. Se actualizaron las reglas para mejorar la detección.	2023-10-11

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado de entradas incorrectas conocidas • `ExploitablePaths_URIPATH`	Implementación de excepción: publicada la versión estática 1.19 de este grupo de reglas. Se actualizó la versión predeterminada para usar la versión 1.19. Se actualizó la regla `ExploitablePaths_URIPATH` para agregar la detección de las solicitudes que coincidan con la vulnerabilidad de escalamiento de privilegios CVE-2023-22515 de Atlassian Confluence. Esta vulnerabilidad afecta a algunas versiones de Atlassian Confluence. Para obtener más información, consulte NIST: National Vulnerability Database: CVE-2023-22515 Detail y Atlassian Support: FAQ for CVE-2023-22515. Para obtener información sobre este tipo de implementación, consulte Implementaciones de excepciones para las reglas administradas de AWS.	2023-10-04

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado de entradas incorrectas conocidas • `Host_localhost_HEADER` • `Log4J*` • `JavaDeserialization*`	Implementación de excepción: publicada la versión estática 1.18 de este grupo de reglas. Se trata de una implementación rápida de esta versión estática para adaptarla a la creación e implementación de la versión 1.19. Se actualizaron la regla `Host_localhost_HEADER` y todas las reglas de deserialización de Log4J y Java para mejorar la detección. Para obtener información sobre este tipo de implementación, consulte Implementaciones de excepciones para las reglas administradas de AWS.	2023-10-04

Reglas y grupos de reglas	Descripción	Fecha
AWS WAF Grupo de reglas de control de bots • `TGT_TokenReuseIp` • `TGT_ML_CoordinatedActivityMedium` • `TGT_ML_CoordinatedActivityHigh`	Se agregaron reglas al grupo de reglas con la acción Count. La regla de IP de reutilización de tokens detecta y cuenta el uso compartido de tokens entre direcciones IP. Las reglas de actividad coordinada utilizan un análisis automatizado del tráfico del sitio web mediante machine learning (ML) para detectar la actividad relacionada con los bots. En la configuración del grupo de reglas, puede desactivar el uso de ML. Con esta versión, los clientes que actualmente utilizan el nivel de protección específicas optan por el uso del ML. Al excluirse , se deshabilitan las reglas de actividad coordinada.	2023-09-06
AWS WAF Grupo de reglas de control de bots • `CategoryAI`	Se agregó la regla `CategoryAI` al grupo de reglas.	2023-08-30

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado del conjunto de reglas básicas (CRS) • `RestrictedExtensions_URIPATH` • `RestrictedExtensions_QUERYARGUMENTS` • `EC2MetaDataSSRF_COOKIE` • `EC2MetaDataSSRF_QUERYARGUMENTS` • `EC2MetaDataSSRF_BODY` • `EC2MetaDataSSRF_URIPATH`	Se lanzó la versión estática 1.7 de este grupo de reglas. Se actualizaron las reglas SSRF de metadatos de EC2 y extensiones restringidas para mejorar la detección y reducir los falsos positivos.	2023-07-26
AWS WAF Grupo de reglas de prevención del fraude (ACFP) para la creación de cuentas de Control de Fraude Todas las reglas están en un nuevo grupo de reglas	Se agregó el grupo de reglas de `AWSManagedRulesACFPRuleSet` .	2023-06-13

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado del sistema operativo Linux • `LFI_HEADER` • `LFI_URIPATH` • `LFI_QUERYSTRING`	Se lanzó la versión estática 2.2 de este grupo de reglas. Se agregaron firmas para mejorar la detección.	2023-05-22
Grupo de reglas administrado del conjunto de reglas básicas (CRS) • `RestrictedExtensions_URIPATH` • `RestrictedExtensions_QUERYARGUMENTS` • `CrossSiteScripting_COOKIE` • `CrossSiteScripting_QUERYARGUMENTS` • `CrossSiteScripting_BODY` • `CrossSiteScripting_URIPATH`	Se lanzó la versión estática 1.6 de este grupo de reglas. Se actualizaron el scripting entre sitios (XSS) y las reglas de extensiones restringidas para mejorar la detección y reducir los falsos positivos.	2023-04-28

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado de la aplicación PHP • Se ha actualizado `PHPHighRiskMethodsVariables_BODY` • Se ha eliminado `PHPHighRiskMethodsVariables_QUERYARGUMENTS` • Se ha agregado `PHPHighRiskMethodsVariables_QUERYSTRING` • Se ha agregado `PHPHighRiskMethodsVariables_HEADER`	Se lanzó la versión estática 2.0 de este grupo de reglas. Se agregaron firmas para mejorar la detección en todas las reglas. Se reemplazó la regla `PHPHighRiskMethodsVariables_QUERYARGUMENTS` por `PHPHighRiskMethodsVariables_QUERYSTRING`, que inspecciona toda la cadena de consulta en lugar de solo los argumentos de la consulta. Se agregó la regla `PHPHighRiskMethodsVariables_HEADER` para ampliar la cobertura e incluir todos los encabezados. Se actualizaron las siguientes etiquetas para alinearlas con el etiquetado estándar AWS de las reglas administradas: • Nombre anterior: `PHPHighRiskMethodsVariables_BODY` Nombre nuevo: `PHPHighRiskMethodsVariables_Body` • Nombre anterior: `PHPHighRiskMethods`	27 de febrero de 2023

Reglas y grupos de reglas	Descripción	Fecha
	`Variables_QUERYARGUMENTS` Nombre nuevo: `PHPHighRiskMethodsVariables_QueryString`	
[AWS WAF Grupo de reglas de prevención de apropiación de cuentas (ATP) para el control del fraude] • `VolumetricIpFailedLoginResponseHigh` • `VolumetricSessionFailedLoginResponseHigh`	Se agregaron reglas de inspección de respuestas de inicio de sesión para su uso con CloudFront distribuciones protegidas de Amazon. Estas reglas pueden bloquear nuevos intentos de inicio de sesión desde direcciones IP y sesiones de clientes que recientemente hayan provocado demasiados intentos fallidos de inicio de sesión.	15-02-2021

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado del conjunto de reglas básicas (CRS) • `NoUserAgent_HEADER` • `CrossSiteScripting_COOKIE` • `CrossSiteScripting_QUERYARGUMENTS` • `CrossSiteScripting_BODY` • `CrossSiteScripting_URIPATH`	Se lanzó la versión estática 1.5 de este grupo de reglas. Se actualizaron los filtros de scripting entre sitios (XSS) para mejorar la detección.	2023-01-25

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado del sistema operativo Linux • `LFI_COOKIE` : eliminado • `LFI_HEADER` : agregado • `LFI_URIPATH` • `LFI_QUERYSTRING`	Se lanzó la versión estática 2.1 de este grupo de reglas. Se eliminaron la regla `LFI_COOKIE` y su etiqueta `awswaf:managed:aws:linux-os:LFI_Cookie` , y se sustituyeron por la nueva regla `LFI_HEADER` y su etiqueta `awswaf:managed:aws:linux-os:LFI_Header` . Este cambio amplía la inspección a varios encabezados. Se han agregado transformaciones de texto y firmas a todas las reglas para mejorar la detección.	2022-12-15

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado del conjunto de reglas básicas (CRS) • `NoUserAgent_HEADER` • `CrossSiteScripting_COOKIE` • `CrossSiteScripting_QUERYARGUMENTS` • `CrossSiteScripting_BODY` • `CrossSiteScripting_URIPATH`	Se lanzó la versión estática 1.4 de este grupo de reglas. Se agregó una transformación de texto a `NoUserAgent_HEADER` para eliminar todos los bytes nulos. Se actualizaron los filtros de reglas scripting entre sitios (XSS) para mejorar la detección.	2022-12-05

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado de entradas incorrectas conocidas • `JavaDeserializationRCE_BODY` • `JavaDeserializationRCE_URIPATH` • `JavaDeserializationRCE_HEADER` • `JavaDeserializationRCE_QUERYSTRING` • `Host_localhost_HEADER`	Se lanzó la versión estática 1.17 de este grupo de reglas. Se actualizaron las reglas de deserialización de Java para agregar la detección de las solicitudes que coincidan con la CVE-2022 42889 de Apache, una vulnerabilidad de ejecución remota de código (RCE) presente en las versiones de Apache Commons Text anteriores a la 1.10.0. Para obtener más información, consulte NIST: National Vulnerability Database: CVE-2022-42889 Detail y CVE-2022-42889: Apache Commons Text prior to 1.10.0 allows RCE when applied to untrusted input due to insecure interpolation defaults. Detección mejorada en `Host_localhost_HEADER` .	2022-10-20

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado de entradas incorrectas conocidas • `Log4JRCE_HEADER` • `Log4JRCE_QUERYSTRING` • `Log4JRCE_URIPATH` • `Log4JRCE_BODY`	Se lanzó la versión estática 1.16 de este grupo de reglas. Se eliminaron los falsos positivos AWS identificados en la versión 1.15.	05/10/2022
Grupo de reglas administrado para el sistema operativo POSIX Grupo de reglas administrado de la aplicación PHP WordPress grupo de reglas gestionado por aplicaciones	Se corrigieron los nombres de las etiquetas documentados.	2022-09-19
Grupos de reglas de reputación de IP • `AWSManagedIPDDoSList`	Este cambio no altera la forma en que el grupo de reglas gestiona el tráfico web. Según la información sobre amenazas de Amazon, se agregó una nueva regla con la acción Count para inspeccionar las direcciones IP que participan activamente en actividades de DDoS.	2022-08-30

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado de entradas incorrectas conocidas • Log4JRCE • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URIPATH • Log4JRCE_BODY • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URIPATH • JavaDeserializationRCE_QUERYSTRING • Host_localhost_HEADER • PROPFIND_METHOD	Se lanzó la versión estática 1.15 de este grupo de reglas. Se quitó Log4JRCE y se sustituyó por Log4JRCE_HEADER , Log4JRCE_QUERYSTRING , Log4JRCE_URI y Log4JRCE_BODY , para una monitorización y una gestión más precisas de los falsos positivos. Se agregaron firmas para mejorar la detección y el bloqueo de PROPFIND_METHOD , y todas las reglas JavaDeserializationRCE* y Log4JRCE* . Se han actualizado las etiquetas para corregir el uso de mayúsculas y minúsculas en Host_localhost_HEADER y en todas las reglas JavaDeserializationRCE* . Se corrigió la descripción de JavaDeserializationRCE_HEADER .	2022-08-22

Reglas y grupos de reglas	Descripción	Fecha
AWS WAF Grupo de reglas de prevención de apropiación de cuentas (ATP) para el control del fraude • `UnsupportedCognitoIDP`	Se agregó una regla para impedir el uso del grupo de reglas administrado de prevención de apropiación de cuentas para el tráfico web del grupo de usuarios de Amazon Cognito.	2022-08-11
Grupo de reglas administrado del conjunto de reglas básicas (CRS)	AWS ha programado la caducidad de las versiones `Version_1.2` y `Version_2.0` del grupo de reglas. Las versiones vencerán el 9 de septiembre de 2022. Para obtener más información sobre la caducidad de versiones, consulte Grupos de reglas gestionados versionados.	9 de junio de 2022
Grupo de reglas administrado del conjunto de reglas básicas (CRS) • `GenericLFI_URIPATH` `GenericRFI_URIPATH`	Se lanzó la versión 1.3 de este grupo de reglas. Esta versión actualiza las firmas de coincidencia en las reglas `GenericLFI_URIPATH` y `GenericRFI_URIPATH` para mejorar la detección.	2022-05-24
AWS WAF Grupo de reglas de control de bots • `CategoryEmailClient`	Se agregó la regla `CategoryEmailClient` al grupo de reglas.	2022-04-06

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado de entradas incorrectas conocidas • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URI • JavaDeserializationRCE_QUERYSTRING	Se lanzó la versión 1.14 de este grupo de reglas. Las cuatro reglas JavaDeserializtionRCE pasan al modo Block.	2022-03-31
Grupo de reglas administrado de entradas incorrectas conocidas • JavaDeserializationRCE_HEADER_RC_COUNT • JavaDeserializationRCE_BODY_RC_COUNT • JavaDeserializationRCE_URI_RC_COUNT • JavaDeserializationRCE_QUERYSTRING_RC_COUNT	Se lanzó la versión 1.13 de este grupo de reglas. Se actualizó la transformación del texto para las vulnerabilidades RCE de Spring Core y Cloud Function. Estas reglas están en modo de recuento para recopilar métricas y evaluar los patrones coincidentes. La etiqueta se puede usar para bloquear las solicitudes en una regla personalizada. Se implementará una versión posterior con estas reglas en modo de bloqueo.	2022-03-31

Reglas y grupos de reglas	Descripción	Fecha
Grupo de reglas administrado de entradas incorrectas conocidas • JavaDeserializationRCE_HEADER_RC_COUNT • JavaDeserializationRCE_BODY_RC_COUNT • JavaDeserializationRCE_URI_RC_COUNT • JavaDeserializationRCE_QUERYSTRING_RC_COUNT • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URI • Log4JRCE_BODY • Log4JRCE	Se lanzó la versión 1.12 de este grupo de reglas. Se agregaron firmas para las vulnerabilidades RCE de Spring Core y Cloud Function. Estas reglas están en modo de recuento para recopilar métricas y evaluar los patrones coincidentes. La etiqueta se puede usar para bloquear las solicitudes en una regla personalizada. Se implementará una versión posterior con estas reglas en modo de bloqueo. Se eliminaron las reglas Log4JRCE_HEADER , Log4JRCE_QUERYSTRING , Log4JRCE_URI y Log4JRCE_BODY ,y se sustituyeron por la regla Log4JRCE.	2022-03-30
Grupos de reglas de reputación de IP • AWSManagedReconnaissanceList	Se actualiza la regla de AWSManagedReconnaissanceList para cambiar la acción de contar en bloque.	2022-02-15

Reglas y grupos de reglas	Descripción	Fecha
AWS WAF Grupo de reglas de prevención de apropiación de cuentas (ATP) para el control del fraude Todas las reglas están en un nuevo grupo de reglas	Se agregó el grupo de reglas de `AWSManagedRulesATPRuleSet` .	2022-02-11
Grupo de reglas administrado de entradas incorrectas conocidas • `Log4JRCE` • `Log4JRCE_HEADER` • `Log4JRCE_QUERYSTRING` • `Log4JRCE_URI` • `Log4JRCE_BODY`	Se lanzó la versión 1.9 de este grupo de reglas. Se ha eliminado la regla `Log4JRCE` y se ha sustituido por las reglas `Log4JRCE_HEADER` , `Log4JRCE_QUERYSTRING` , `Log4JRCE_URI` y `Log4JRCE_BODY` para aumentar la flexibilidad en el uso de esta funcionalidad. Se agregaron firmas para mejorar la detección y el bloqueo.	2022-01-28

Reglas y grupos de reglas	Descripción	Fecha
Conjunto de reglas básicas (CRS) • `CrossSiteScripting_URIPATH` • `CrossSiteScripting_BODY` • `CrossSiteScripting_QUERYARGUMENTS` • `CrossSiteScripting_COOKIE`	Se lanzó la versión 2.0 de este grupo de reglas. Para estas reglas, se ajustaron las firmas de detección para reducir los falsos positivos. Se reemplazó la transformación de texto de `URL_DECODE` por la transformación de texto doble de `URL_DECODE_UNI` . Se agregó la transformación de texto de `HTML_ENTITY_DECODE` .	2022-01-10
Conjunto de reglas básicas (CRS) • `RestrictedExtensions_URIPATH` • `RestrictedExtensions_QUERYARGUMENTS`	Como parte del lanzamiento de la versión 2.0 de este grupo de reglas, se agregó la transformación de texto de `URL_DECODE_UNI` . Se ha eliminado la transformación de texto de `URL_DECODE` de `RestrictedExtensions_URIPATH` .	2022-01-10

Reglas y grupos de reglas	Descripción	Fecha
Base de datos SQL • SQLi_BODY • SQLi_QUERYARGUMENTS • SQLi_COOKIE • SQLi_URIPATH • SQLiExtendedPatterns_BODY • SQLiExtendedPatterns_QUERYARGUMENTS	Se lanzó la versión 2.0 de este grupo de reglas. Se reemplazó la transformación de texto de URL_DECODE por la transformación de texto doble de URL_DECODE_UNI y se añadió la transformación de texto de COMPRESS_WHITE_SPACE . Se agregaron más firmas de detección a SQLiExtendedPatterns_QUERYARGUMENTS . Se agregó la inspección JSON a SQLi_BODY . Se agregó la regla SQLiExtendedPatterns_BODY . Se ha eliminado la regla SQLi_URIPATH .	2022-01-10
Entradas incorrectas conocidas • Log4JRCE	Se lanzó la versión 1.8 de la regla Log4JRCE para mejorar la inspección de los encabezados y los criterios de coincidencia.	2021-12-17

Reglas y grupos de reglas	Descripción	Fecha
Entradas incorrectas conocidas • `Log4JRCE`	Se lanzó la versión 1.4 de la regla `Log4JRCE` para mejorar los criterios de coincidencia y la inspección de encabezados adicionales. Se lanzó la versión 1.5 para mejorar los criterios de coincidencia.	2021-12-11
Entradas incorrectas conocidas • `Log4JRCE` • `BadAuthToken_COOKIE_AUTHORIZATION`	Se agregó la versión 1.2 de la regla `Log4JRCE` en respuesta al problema de seguridad recientemente revelado en Log4j. Para obtener información, consulte CVE-2021-44228. Esta regla inspecciona las rutas de URI comunes, las cadenas de consulta, los primeros 8 KB del cuerpo de la solicitud y los encabezados comunes. La regla usa transformaciones de texto dobles de `URL_DECODE_UNI` . Se lanzó la versión 1.3 de la regla `Log4JRCE` para mejorar los criterios de coincidencia y la inspección de encabezados adicionales. Se ha eliminado la regla `BadAuthToken_COOKIE_AUTHORIZATION` .	2021-12-10

En la siguiente tabla, se muestran los cambios realizados antes de diciembre de 2021.

Reglas y grupos de reglas	Descripción	Fecha	
Lista de reputación de IP de Amazon	`AWSManagedReconnaissanceList`	Se agregó la regla `AWSManagedReconnaissanceList` en el modo de monitoreo/recuento. Esta regla contiene direcciones IP que realizan un reconocimiento de los recursos. AWS	2021-11-23
Sistema operativo Windows	`WindowsShellCommands` `PowerShellCommands`	Se agregaron tres nuevas reglas para los WindowsShell comandos: `WindowsShellCommands_COOKIE`, y `WindowsShellCommands_QUERYARGUMENTS`. `WindowsShellCommands_BODY` Se agregó una nueva PowerShell regla: `PowerShellCommands_COOKIE`. Reestructuró la denominación de las	2021-11-23

Reglas y grupos de reglas	Descripción	Fecha	
		reglas `PowerShellComands` eliminando las cadenas _Set1 y _Set2. Se agregaron firmas de detección más completas a `PowerShellRules` . Se agregó la transformación de texto de `URL_DECODE_UNI` a todas las reglas del sistema operativo Windows.	

Reglas y grupos de reglas	Descripción	Fecha	
Sistema operativo Linux	`LFI_URIPATH` `LFI_QUERYSTRING` `LFI_BODY` `LFI_COOKIE`	Se reemplazó la transformación de texto doble de `URL_DECODE` por `URL_DECODE_UNI` doble. Se agregó `NORMALIZE _PATH_WIN` como segunda transform ación de texto. Se reemplazó la regla `LFI_BODY` por la regla `LFI_COOKIE` . Se agregaron firmas de detección más completas para todas las reglas de `LFI`.	2021-11-23
Conjunto de reglas básicas (CRS)	`SizeRestr ictions_BODY`	Se ha reducido el límite de tamaño para bloquear las solicitud es web con cargas de cuerpo de más de 8 KB. Anteriormente, el límite era de 10 KB.	2021-10-27

Reglas y grupos de reglas	Descripción	Fecha	
Conjunto de reglas básicas (CRS)	`EC2MetaDataSSRF_BODY` `EC2MetaDataSSRF_COOKIE` `EC2MetaDataSSRF_URIPATH` `EC2MetaDataSSRF_QUERYARGUMENTS`	Se agregaron más firmas de detección. Se ha agregado una doble decodificación de URL unicode para mejorar el bloqueo.	2021-10-27
Conjunto de reglas básicas (CRS)	`GenericLFI_QUERYARGUMENTS` `GenericLFI_URIPATH` `RestrictedExtensions_URIPATH` `RestrictedExtensions_QUERYARGUMENTS`	Se ha agregado una doble decodificación de URL unicode para mejorar el bloqueo.	2021-10-27

Reglas y grupos de reglas	Descripción	Fecha	
Conjunto de reglas básicas (CRS)	`GenericRFI_QUERYARGUMENTS` `GenericRFI_BODY` `GenericRFI_URIPATH`	Se actualizaron las firmas de reglas para reducir los falsos positivos en función de los comentarios de los clientes. Se ha agregado una doble decodificación de URL unicode para mejorar el bloqueo.	2021-10-27
Todos	Todas las reglas	Se agregó la compatibilidad con AWS WAF etiquetas a todas las reglas que aún no lo admitían.	2021-10-25
Lista de reputación de IP de Amazon	`AWSManagedIPReputationList_xxxx`	Se reestructuró la lista de reputación IP, se eliminaron los sufijos del nombre de la regla y se agregó compatibilidad con las etiquetas . AWS WAF	04/05/2021
Lista de IP anónimas	`AnonymousIPList` `HostingProviderList`	Se agregó soporte para etiquetas. AWS WAF	04/05/2021
Control de bots	Todos	Se agregó el conjunto de reglas de control de bots.	2021-04-01

Reglas y grupos de reglas	Descripción	Fecha	
Conjunto de reglas básicas (CRS)	`GenericRFI_QUERYARGUMENTS`	Se ha agregado una doble decodificación de URL.	2021-03-03
Conjunto de reglas básicas (CRS)	`RestrictedExtensions_URIPATH`	Se mejoró la configuración de las reglas y se agregó una decodificación de URL adicional.	2021-03-03
Protección de administración	`AdminProtection_URIPATH`	Se ha agregado una doble decodificación de URL.	2021-03-03
Entradas incorrectas conocidas	`ExploitablePaths_URIPATH`	Se mejoró la configuración de las reglas y se agregó una decodificación de URL adicional.	2021-03-03
Sistema operativo Linux	`LFI_QUERYARGUMENTS`	Se mejoró la configuración de las reglas y se agregó una decodificación de URL adicional.	2021-03-03
Sistema operativo Windows	Todos	Se ha mejorado la configuración de las reglas.	2020-09-23

Reglas y grupos de reglas	Descripción	Fecha	
Aplicaciones PHP	`PHPHighRiskMethodsVariables_QUERYARGUMENTS` `PHPHighRiskMethodsVariables_BODY`	Se ha cambiado la transformación de texto de la decodificación de HTML a la decodificación de URL, para mejorar el bloqueo.	2020-09-16
Sistema operativo POSIX	`UNIXShellCommandsVariables_QUERYARGUMENTS` `UNIXShellCommandsVariables_BODY`	Se ha cambiado la transformación de texto de la decodificación de HTML a la decodificación de URL, para mejorar el bloqueo.	2020-09-16
Conjunto de reglas básicas	`GenericLFI_QUERYARGUMENTS` `GenericLFI_URIPATH` GenericLFI_BODY	Se ha cambiado la transformación de texto de la decodificación de HTML a la decodificación de URL, para mejorar el bloqueo.	2020-08-07

Reglas y grupos de reglas	Descripción	Fecha	
Sistema operativo Linux	`LFI_URIPATH` `LFI_QUERY ARGUMENTS` `LFI_BODY`	Se ha cambiado la transformación de texto de la decodific ación de entidades HTML a la decodific ación de URL, para mejorar la detección y el bloqueo.	2020-05-19
Lista de direcciones IP anónimas	Todos	Nuevo grupo de reglas en Grupos de reglas de reputación de IP para bloquear solicitudes de servicios que permiten ocultar la identidad del lector, para ayudar a mitigar los bots y para evadir las restricciones geográficas.	2020-03-06
WordPress solicitud	`WordPress Exploitab leCommand s_QUERYSTRING`	Nueva regla que comprueba si hay comandos vulnerabl es en la cadena de consulta.	2020-03-03

Reglas y grupos de reglas	Descripción	Fecha	
Conjunto de reglas básicas (CRS)	`SizeRestrictions_QUERYSTRING` `SizeRestrictions_Cookie_HEADER` `SizeRestrictions_BODY` `SizeRestrictions_URIPATH`	Se han ajustado las restricciones de valor de tamaño para mejorar la precisión.	2020-03-03
Base de datos SQL	`SQLi_URIPATH`	Las reglas ahora comprueban el URI del mensaje.	2020-01-23
Base de datos SQL	`SQLi_BODY` `SQLi_QUERYARGUMENTS` `SQLi_COOKIE`	Transformaciones de texto actualizadas.	2019-12-20

Reglas y grupos de reglas	Descripción	Fecha	
Conjunto de reglas básicas (CRS)	`CrossSite Scripting _URIPATH` `CrossSite Scripting_BODY` `CrossSite Scripting _QUERYARG UMENTS` `CrossSite Scripting _COOKIE`	Transformaciones de texto actualizadas.	2019-12-20

AWS Marketplace grupos de reglas gestionados

AWS Marketplace Los grupos de reglas gestionados están disponibles mediante suscripción a través de la AWS Marketplace consola en AWS Marketplace. Después de suscribirse a un grupo de reglas AWS Marketplace administrado, puede usarlo en AWS WAF. Para usar un grupo de AWS Marketplace reglas en una AWS Firewall Manager AWS WAF política, todas las cuentas de la organización deben suscribirse a él.

Pruebe y ajuste cualquier cambio en sus AWS WAF protecciones antes de utilizarlas para el tráfico de producción. Para obtener más información, consulte Probando y ajustando sus AWS WAF protecciones.

AWS Marketplace Precios por grupos de reglas

AWS Marketplace Los grupos de reglas están disponibles sin contratos a largo plazo ni compromisos mínimos. Si se suscribe a un grupo de reglas, se le cobrará una cuota mensual (prorrateada por hora) y cuotas continuas de solicitudes en función del volumen. Para obtener más información, consulte AWS WAF los precios y la descripción de cada grupo de AWS Marketplace reglas en AWS Marketplace.

¿Tiene alguna pregunta sobre un grupo de AWS Marketplace reglas?

Si tienes preguntas sobre un grupo de reglas gestionado por un AWS Marketplace vendedor y si deseas solicitar cambios en su funcionalidad, ponte en contacto con el equipo de atención al cliente del proveedor. Para encontrar la información de contacto, consulte el listado del proveedor en AWS Marketplace.

El proveedor del grupo de AWS Marketplace reglas determina cómo administrar el grupo de reglas, por ejemplo, cómo actualizar el grupo de reglas y si el grupo de reglas está versionado. El proveedor también determina los detalles del grupo de reglas, incluidas las reglas, las acciones de reglas y cualquier etiqueta que las reglas agreguen a las solicitudes web coincidentes.

Suscribirse a grupos de reglas AWS Marketplace administrados

Puede suscribirse y cancelar su suscripción a los grupos de AWS Marketplace reglas en la AWS WAF consola.

> **Important**
>
> Para usar un grupo de AWS Marketplace reglas en una AWS Firewall Manager política, cada cuenta de la organización debe suscribirse primero a ese grupo de reglas.

Para suscribirse a un grupo de reglas AWS Marketplace administrado

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, elija AWS Marketplace.
3. En la sección Available marketplace products, elija el nombre de un grupo de reglas para ver los detalles y la información sobre precios.
4. Si desea suscribirse al grupo de reglas, elija Continue.

   > **Note**
   >
   > Si no desea suscribirse a este grupo de reglas, solo tiene que cerrar esta página en su navegador.

5. Elija Set up your account.

6. Agregue el grupo de reglas a una ACL web, de forma similar a la forma en que agrega una regla individual. Para obtener más información, consulte Crear una ACL web o Edición de una ACL web.

> **Note**
>
> Al agregar un grupo de reglas a una ACL web, puede anular las acciones de las reglas del grupo de reglas y el resultado del grupo de reglas. Para obtener más información, consulte Opciones de anulación de acciones para grupos de reglas.

Después de suscribirse a un grupo de AWS Marketplace reglas, lo usa en sus ACL web como lo hace con otros grupos de reglas administrados. Para obtener más información, consulte Crear una ACL web.

Cancelar la suscripción a los grupos de reglas administrados AWS Marketplace

Puede darse de baja de los grupos de AWS Marketplace reglas en la AWS WAF consola.

> **Important**
>
> Para detener los cargos de suscripción de un grupo de reglas AWS Marketplace administrado, debe eliminarlo de todas las ACL web incluidas en cualquier AWS WAF política de Firewall Manager AWS WAF y cancelar la suscripción a él. Si cancela la suscripción a un grupo de reglas AWS Marketplace administrado pero no lo elimina de sus ACL web, se le seguirá cobrando la suscripción.

Para cancelar la suscripción a un grupo de reglas AWS Marketplace administrado

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.
2. Quite el grupo de reglas de todas las ACL web. Para obtener más información, consulte Edición de una ACL web.
3. En el panel de navegación, elija AWS Marketplace.
4. Elija Manage your subscriptions.
5. Elija Cancel subscription situada junto al nombre del grupo de reglas cuya suscripción desea cancelar.

6. Elija Yes, cancel subscription.

Solución de problemas de grupos de AWS Marketplace reglas

Si descubre que un grupo de AWS Marketplace reglas bloquea el tráfico legítimo, puede solucionar el problema siguiendo estos pasos.

Para solucionar problemas de un grupo de reglas de AWS Marketplace

1. Anule las acciones de recuento de las reglas que bloquean el tráfico legítimo. Puede identificar qué reglas bloquean solicitudes específicas mediante las solicitudes AWS WAF muestreadas o AWS WAF los registros. Puede identificar las reglas si consulta el campo `ruleGroupId` en el registro o la regla `RuleWithinRuleGroup` en la solicitud muestreada. Puede identificar la regla en el patrón de `<Seller Name>#<RuleGroup Name>#<Rule Name>`.
2. Si establecer reglas específicas para que solo cuenten las solicitudes no resuelve el problema, puedes anular todas las acciones de la regla o cambiar la acción del propio grupo de AWS Marketplace reglas de No anular a anular el recuento. Esto permite el paso de la solicitud web, independientemente de las acciones de las reglas individuales incluidas en el grupo de reglas.
3. Tras anular la acción de la regla individual o toda la acción del grupo de AWS Marketplace reglas, ponte en contacto con el equipo de atención al cliente del proveedor del grupo de reglas para seguir solucionando el problema. Para obtener información de contacto, consulte la lista de grupos de reglas en las páginas de listas de productos en AWS Marketplace.

Contactar con el soporte AWS

Si tiene problemas con AWS WAF un grupo de reglas gestionado por él AWS, póngase en contacto con AWS Support. Si tienes problemas con un grupo de reglas gestionado por un AWS Marketplace vendedor, ponte en contacto con el equipo de atención al cliente del proveedor. Para encontrar la información de contacto, consulta el listado del proveedor en AWS Marketplace.

Administrar sus propios grupos de reglas

Puede crear su propio grupo de reglas para reutilizar conjuntos de reglas que no encuentre en las ofertas de grupos de reglas administrados o para gestionarlos por cuenta propia si así lo prefiere.

Los grupos de reglas que cree tienen reglas, al igual que una ACL web, y estas se agregan como si se tratase de una ACL web. Al crear su propio grupo de reglas, tiene que establecer una capacidad máxima inmutable para él.

Temas

Crear un grupo de reglas

Para crear un grupo de reglas nuevo, siga el procedimiento de esta página.

Para crear un grupo de reglas

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, elija Rule Groups (Grupos de reglas) y, a continuación, Create rule group (Crear grupo de reglas).
3. Introduzca un nombre y una descripción del grupo. Los usará para identificar el conjunto de reglas y así administrarlo y usarlo.

   No utilice nombres que comiencen por `AWS`, `Shield`, `PreFM` o `PostFM`. Estas cadenas están reservadas o pueden causar confusión con los grupos de reglas que otros servicios administran para usted. Consulte Grupos de reglas proporcionados por otros servicios.

   > **Note**
   >
   > No se puede cambiar el nombre después de crear el grupo.

4. En Region (Región), elija la región en la que quiera almacenar el grupo de reglas. Para usar un grupo de reglas en las ACL web que protegen CloudFront las distribuciones de Amazon, debes usar la configuración global. También puede usar la configuración global para aplicaciones regionales.
5. Elija Siguiente.
6. Agregue reglas al grupo de reglas mediante el asistente Rule builder (Generador de reglas) al igual que en la gestión de una ACL web. La única diferencia es que no se puede agregar un grupo de reglas a otro grupo de reglas.

7. En Capacity (Capacidad), establezca el máximo de uso que el grupo de reglas puede hacer de las unidades de capacidad de ACL web (WCU). Se trata de una configuración inmutable. Para obtener información acerca de las WCU, consulte AWS WAF unidades de capacidad ACL web (WCU).

   A medida que agrega reglas al grupo, el panel Add rules and set capacity (Añadir reglas y establecer capacidad) muestra la capacidad mínima requerida, que se basa en las reglas que ya ha agregado. Puede utilizar este y sus planes futuros para el grupo de reglas para hacer una estimación de la capacidad que necesitará el grupo de reglas.
8. Revise la configuración del grupo de reglas y seleccione Create (Crear).

Edición de un grupo de reglas

Para agregar o eliminar reglas de un grupo de reglas o cambiar los ajustes de configuración, acceda al grupo de reglas mediante el procedimiento de esta página.

> ⚠ Riesgo de tráfico de producción
>
> Si cambia un grupo de reglas que está utilizando actualmente en una ACL web, esos cambios afectarán al comportamiento de la ACL web independientemente de dónde se utilice. Asegúrese de probar y ajustar todos los cambios en un entorno de ensayo o pruebas hasta que se sienta cómodo con el impacto potencial en su tráfico. A continuación, pruebe y ajuste las reglas actualizadas en el modo de recuento con el tráfico de producción antes de habilitarlas. Para obtener instrucciones, consulte Probando y ajustando sus AWS WAF protecciones.

Edición de un grupo de reglas

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, elija Rule groups (Grupos de reglas).
3. Elija el nombre del grupo de reglas que desea editar. La consola lo lleva a la página del grupo de reglas.
4. Edite el grupo de reglas según sea necesario. Puede editar las propiedades mutables del grupo de reglas, de forma similar a como lo hizo durante la creación. La consola guarda los cambios sobre la marcha.

> **Note**
>
> Si cambias el nombre de una regla y quieres que el nombre de la métrica de la regla refleje el cambio, también debes actualizar el nombre de la métrica. AWS WAF no actualiza automáticamente el nombre de la métrica de una regla cuando se cambia el nombre de la regla. Puede cambiar el nombre de la métrica al editar la regla en la consola mediante el editor de reglas de JSON. También puede cambiar ambos nombres a través de las API y en cualquier lista de JSON que utilice para definir su ACL web o grupo de reglas.

Incoherencias temporales durante las actualizaciones

Al crear o cambiar una ACL web u otros AWS WAF recursos, los cambios tardan un poco en propagarse a todas las áreas donde se almacenan los recursos. El tiempo de propagación puede oscilar entre unos segundos y varios minutos.

A continuación, se proporcionan ejemplos de incoherencias temporales que podría notar durante la propagación de los cambios:

- Después de crear una ACL web, si intenta asociarla a un recurso, es posible que se produzca una excepción que indique que la ACL web no está disponible.
- Después de agregar un grupo de reglas a una ACL web, las nuevas reglas del grupo de reglas pueden estar en vigor en un área en la que se usa la ACL web y no en otra.
- Tras cambiar la configuración de una acción de regla, es posible que vea la acción anterior en algunos lugares y la acción nueva en otros.
- Después de agregar una dirección IP a un conjunto de IP que está en uso dentro de una regla de bloqueo, es posible que la nueva dirección se bloquee en un área, pero que se permita en otra.

Uso del grupo de reglas en una ACL web

Para usar un grupo de reglas en una ACL web, agréguelo a la ACL web en una instrucción de referencia del grupo de reglas.

Riesgo de tráfico de producción

Antes de implementar cambios en su ACL web para el tráfico de producción, pruébelos y ajústelos en un entorno provisional o de pruebas hasta que se sienta cómodo con el posible impacto en el tráfico. A continuación, pruebe y ajuste las reglas actualizadas en el modo de recuento con el tráfico de producción antes de habilitarlas. Para obtener instrucciones, consulte Probando y ajustando sus AWS WAF protecciones.

Note

El uso de más de 1500 WCU en una ACL web conlleva costos superiores al precio de la ACL web básica. Para obtener más información, consulte AWS WAF unidades de capacidad ACL web (WCU) y Precios de AWS WAF.

En la consola, cuando agregue o actualice las reglas en la ACL web, vaya a la página Añadir reglas y grupos de reglas, seleccione Añadir reglas y, a continuación, elija Añadir mis propias reglas y grupos de reglas. A continuación, seleccione Rule group (Grupo de reglas) y seleccione el grupo de reglas de la lista.

En su ACL web, puede modificar el comportamiento de un grupo de reglas y sus reglas configurando las acciones de reglas individuales en Count o cualquier otra acción. Esto puede ayudarle a realizar tareas como probar un grupo de reglas, identificar los falsos positivos de las reglas de un grupo de reglas y personalizar la forma en que un grupo de reglas administrado gestiona sus solicitudes. Para obtener más información, consulte Opciones de anulación de acciones para grupos de reglas.

Si su grupo de reglas contiene una instrucción basada en tasas, cada ACL web en la que utilice el grupo de reglas tiene su propio seguimiento y administración de tasas independiente para la regla basada en tasas, sin importar cualquier otra ACL web en la que utilice el grupo de reglas. Para obtener más información, consulte Instrucción de regla basada en frecuencia.

Incoherencias temporales durante las actualizaciones

Al crear o cambiar una ACL web u otros AWS WAF recursos, los cambios tardan un poco en propagarse a todas las áreas donde se almacenan los recursos. El tiempo de propagación puede oscilar entre unos segundos y varios minutos.

A continuación, se proporcionan ejemplos de incoherencias temporales que podría notar durante la propagación de los cambios:

- Después de crear una ACL web, si intenta asociarla a un recurso, es posible que se produzca una excepción que indique que la ACL web no está disponible.
- Después de agregar un grupo de reglas a una ACL web, las nuevas reglas del grupo de reglas pueden estar en vigor en un área en la que se usa la ACL web y no en otra.
- Tras cambiar la configuración de una acción de regla, es posible que vea la acción anterior en algunos lugares y la acción nueva en otros.
- Después de agregar una dirección IP a un conjunto de IP que está en uso dentro de una regla de bloqueo, es posible que la nueva dirección se bloquee en un área, pero que se permita en otra.

Compartir un grupo de reglas con otra cuenta

Puede compartir un grupo de reglas de su propiedad con otra AWS cuenta para que lo use esa cuenta. Solo puedes hacerlo a través de la AWS WAF API. Para obtener más información, consulta PutPermissionPolicyla referencia de la AWS WAF API.

Eliminar un grupo de reglas

Siga las instrucciones que se detallan en esta sección para eliminar un grupo de reglas.

Eliminación de conjuntos o grupos de reglas al que se hace referencia

Al eliminar una entidad que puede usar en una ACL web, como un conjunto de IP, un conjunto de patrones de expresiones regulares o un grupo de reglas, AWS WAF comprueba si la entidad se está utilizando actualmente en una ACL web. Si descubre que está en uso, AWS WAF le avisa. AWS WAF casi siempre puede determinar si una ACL web está haciendo referencia a una entidad. No obstante, es posible que en algunos casos no consiga hacerlo. Si tiene que asegurarse de que no hay nada que esté utilizando actualmente la entidad, verifique sus ACL de la web antes de eliminarla. Si la entidad es un conjunto al que se hace referencia, verifique que ningún grupo de reglas la esté utilizando.

Para eliminar un grupo de reglas:

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, elija Rule groups (Grupos de reglas).

3. Seleccione el grupo de reglas que desea eliminar y, a continuación, haga clic en Delete (Eliminar).

Grupos de reglas proporcionados por otros servicios

Si usted o un administrador de su organización utilizan AWS Firewall Manager o AWS Shield Advanced administran las protecciones de recursos mediante AWS WAF, es posible que vea declaraciones de referencia de grupos de reglas agregadas a las ACL web de su cuenta.

Los nombres de estos grupos de reglas comienzan con las siguientes cadenas:

- **`ShieldMitigationRuleGroup`**— Estos grupos de reglas se administran AWS Shield Advanced y utilizan para mitigar automáticamente los ataques DDoS en la capa de aplicación para proteger los recursos de la capa de aplicaciones (capa 7).

  Al habilitar la mitigación automática de DDoS de la capa de aplicación para un recurso protegido, Shield Advanced agrega uno de estos grupos de reglas a la ACL web que ha asociado al recurso. Shield Advanced asigna a la instrucción de referencia del grupo de reglas una configuración de prioridad de 10 000 000, de modo que se ejecute según las reglas que haya configurado en la ACL web. Para obtener más información acerca de estos grupos de reglas, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced.

  > **Warning**
  >
  > No intente administrar manualmente este grupo de reglas en su ACL web. En particular, no elimine manualmente la instrucción de referencia del grupo de reglas de `ShieldMitigationRuleGroup` de su ACL web. Hacerlo podría tener consecuencias imprevistas para todos los recursos asociados a la ACL web. En su lugar, utilice Shield Advanced para deshabilitar la mitigación automática de los recursos asociados a la ACL web. Shield Advanced eliminará el grupo de reglas por usted cuando no sea necesario para la mitigación automática.

- **`PREFMManaged`**y **`POSTFMManaged`** — Estos grupos de reglas son administrados por AWS Firewall Manager. Firewall Manager los proporciona dentro de las ACL web que Firewall Manager crea y administra. Los nombres de las ACL web comienzan por `FMManagedWebACLV2`. Para obtener información acerca de estas ACL web y los grupos de reglas, consulte AWS WAF políticas.

AWS WAF reglas

Una AWS WAF regla define cómo inspeccionar las solicitudes web HTTP (S) y la acción que se debe realizar cuando una solicitud coincide con los criterios de inspección. Defina las reglas únicamente en el contexto de una ACL web o un grupo de reglas.

Las reglas no existen AWS WAF por sí solas. No son AWS recursos y no tienen nombres de recursos de Amazon (ARN). Puede acceder a una regla por su nombre en el grupo de reglas o en la ACL web donde está definida. Para administrar reglas y copiarlas en otras ACL web, use la vista JSON del grupo de reglas o ACL web que contiene la regla. También puede administrarlos mediante el generador de reglas de la AWS WAF consola, que está disponible para las ACL web y los grupos de reglas.

Nombre de la regla

Cada regla requiere un nombre. Evite los nombres que comiencen por `AWS` y los nombres que se usen para grupos de reglas o reglas que otros servicios administren para usted. Consulte Grupos de reglas proporcionados por otros servicios.

> **Note**
>
> Si cambia el nombre de una regla y desea que el nombre de la métrica de la regla refleje el cambio, también debe actualizar el nombre de la métrica. AWS WAF no actualiza automáticamente el nombre de la métrica de una regla cuando se cambia el nombre de la regla. Puede cambiar el nombre de la métrica al editar la regla en la consola mediante el editor de reglas de JSON. También puede cambiar ambos nombres a través de las API y en cualquier lista de JSON que utilice para definir su ACL web o grupo de reglas.

Instrucción de reglas

Cada regla también requiere una instrucción de regla que defina cómo la regla inspecciona las solicitudes web. Cada regla requiere una instrucción de nivel superior, que puede contener instrucciones anidadas a cualquier profundidad, en función del tipo de regla y de instrucción. Algunas instrucciones de reglas toman conjuntos de criterios. Por ejemplo, puede especificar hasta 10 000 direcciones IP o rangos de direcciones de IP en una regla de coincidencia de IP.

Puede definir reglas que inspeccionen criterios como los siguientes:

- Scripts que probablemente sean maliciosos. Los atacantes incrustan scripts que pueden aprovechar vulnerabilidades en aplicaciones web. Esto es lo que se conoce como scripting entre sitios (XSS).
- Direcciones IP o rangos de direcciones de las que procedan las solicitudes.
- País o ubicación geográfica de donde provienen las solicitudes.
- Longitud de la parte especificada de la solicitud, como la cadena de consulta.
- Código SQL que puede ser malicioso. Los atacantes tratan de extraer los datos de su base de datos incrustando código SQL malicioso en una solicitud web. Esto es lo que se conoce como inyección de código SQL.
- Cadenas que aparecen en la solicitud, por ejemplo, valores que aparecen en el encabezado de `User-Agent` o cadenas de texto que aparecen en la cadena de consulta. También puede utilizar expresiones regulares (regex) para especificar estas cadenas.
- Etiquetas que las reglas anteriores de la ACL web agregaron a la solicitud.

Además de las instrucciones con criterios de inspección de solicitudes web, como las de la lista anterior, AWS WAF admite las instrucciones lógicas y `NOT` que se utilizan para combinar las instrucciones de una regla. `AND` `OR`

Por ejemplo, en función de las últimas solicitudes que haya visto de un atacante, puede crear una regla con una instrucción `AND` lógica que incluya las siguientes instrucciones anidadas:

- Las solicitudes provienen de 192.0.2.44.
- Contienen el valor `BadBot` en el encabezado `User-Agent`.
- Parece que incluyan código tipo SQL en la cadena de consulta.

En este caso, todas las instrucciones tienen que dar como resultado una coincidencia para que la instrucción `AND` de nivel superior coincida.

Temas

- Acción de regla
- Conceptos básicos de las instrucciones de regla
- instrucciones de coincidencia
- instrucciones de reglas lógicas
- Instrucción de regla basada en frecuencia

- Instrucciones de regla de grupos de reglas

Acción de regla

La acción de la regla indica AWS WAF qué hacer con una solicitud web cuando coincide con los criterios definidos en la regla. Si lo desea, puede agregar un comportamiento personalizado a cada acción de regla.

> **Note**
>
> Las acciones de la regla pueden ser de finalización o no. Una acción de finalización detiene la evaluación de la solicitud por parte de la ACL web y permite que continúe con la aplicación protegida o la bloquea.

Estas son las opciones de la acción de la regla:

- Allow— AWS WAF permite reenviar la solicitud al AWS recurso protegido para su procesamiento y respuesta. Se trata de una acción de finalización. En las reglas que defina, puede insertar encabezados personalizados en la solicitud antes de reenviarla al recurso protegido.
- Block— AWS WAF bloquea la solicitud. Se trata de una acción de finalización. De forma predeterminada, el AWS recurso protegido responde con un código de `403 (Forbidden)` estado HTTP. En las reglas que defina, puede personalizar la respuesta. Cuando AWS WAF bloquea una solicitud, la configuración de la Block acción determina la respuesta que el recurso protegido envía al cliente.
- Count— AWS WAF cuenta la solicitud pero no determina si se permite o se bloquea. Se trata de una acción no terminal. AWS WAF continúa procesando las reglas restantes en la ACL web. En las reglas que defina, puede insertar encabezados personalizados en la solicitud y puede agregar etiquetas con las que puedan coincidir otras reglas.
- CAPTCHAy Challenge: AWS WAF usa acertijos CAPTCHA y desafíos silenciosos para verificar que la solicitud no proviene de un bot, y AWS WAF usa fichas para rastrear las respuestas recientes de los clientes que han obtenido buenos resultados.

  Los acertijos de CAPTCHA y los desafíos silenciosos solo se pueden ejecutar cuando los navegadores acceden a los puntos finales HTTPS. Los clientes del navegador deben ejecutarse en contextos seguros para poder adquirir los tokens.

> **Note**
>
> Se le cobrarán tarifas adicionales cuando utilice la acción de regla CAPTCHA o Challenge en una de sus reglas o como anulación de una acción de regla en un grupo de reglas. Para obtener más información, consulte AWS WAF Precios.

Estas acciones de regla pueden ser de finalización o no, según el estado del token de la solicitud:

- No se cancela para un token válido y no caducado: si el token es válido y no ha caducado según el CAPTCHA configurado o el tiempo de inmunidad de impugnación, AWS WAF gestiona la solicitud de forma similar a la acción. Count AWS WAF continúa inspeccionando la solicitud web en función de las demás reglas de la ACL web. Al igual que en la configuración de Count, en las reglas que defina, puede configurar opcionalmente estas acciones con encabezados personalizados para insertarlos en la solicitud y puede agregar etiquetas con las que puedan coincidir otras reglas.
- Finalizar con una solicitud bloqueada de un token no válido o caducado: si el token no es válido o la marca de tiempo indicada ha caducado, AWS WAF finaliza la inspección de la solicitud web y bloquea la solicitud, de forma similar a como se ha hecho antes. Block AWS WAF a continuación, responde al cliente con un código de respuesta personalizado. PuesCAPTCHA, si el contenido de la solicitud indica que el navegador del cliente puede gestionarla, AWS WAF envía un acertijo CAPTCHA en un JavaScript intersticial, diseñado para distinguir a los clientes humanos de los bots. Para elloChallenge, AWS WAF envía un JavaScript intersticial con un desafío silencioso diseñado para distinguir los navegadores normales de las sesiones ejecutadas por bots.

Para obtener información adicional, consulte CAPTCHAy Challenge en AWS WAF.

Para obtener información sobre cómo personalizar las solicitudes y las respuestas, consulte Solicitudes web y respuestas personalizadas en AWS WAF.

Para obtener información sobre cómo agregar etiquetas a las solicitudes coincidentes, consulte AWS WAF etiquetas en las solicitudes web.

Para obtener información acerca de cómo interactúan la ACL web y la configuración de reglas, consulte Evaluación de reglas y grupos de reglas de ACL web.

Conceptos básicos de las instrucciones de regla

Las declaraciones de reglas son la parte de una regla que indica AWS WAF cómo inspeccionar una solicitud web. Cuando AWS WAF encuentra los criterios de inspección en una solicitud web, decimos que la solicitud web coincide con la declaración. Cada declaración de regla especifica qué buscar y cómo, según el tipo de declaración.

Cada regla AWS WAF tiene una única declaración de regla de nivel superior, que puede contener otras declaraciones. Las declaraciones de reglas pueden ser muy sencillas. Por ejemplo, podría tener una instrucción que proporcione un conjunto de países originarios para inspeccionar sus solicitudes web o podría tener una instrucción de regla en una ACL web que solo haga referencia a un grupo de reglas. Las declaraciones de reglas también pueden ser muy complejas. Por ejemplo, podría tener una instrucción que combine muchas otras instrucciones con instrucciones lógicas AND, OR y NOT.

Para la mayoría de las reglas, puedes añadir un AWS WAF etiquetado personalizado a las solicitudes coincidentes. Las reglas de los grupos de reglas de reglas AWS administradas agregan etiquetas a las solicitudes coincidentes. Las etiquetas que agrega una regla proporcionan información sobre la solicitud a las reglas que se evalúan más adelante en la ACL web y también en AWS WAF los registros y las métricas. Para obtener información sobre el etiquetado, consulte AWS WAF etiquetas en las solicitudes web yInstrucción de regla de coincidencia de etiquetas.

Declaraciones de reglas de anidamiento

AWS WAF admite la anidación para muchas declaraciones de reglas, pero no para todas. Por ejemplo, no se puede anidar una instrucción de grupo de reglas dentro de otra instrucción. Es necesario utilizar la anidación en algunos escenarios, como las instrucciones de restricción de acceso y las instrucciones lógicas. Las listas de instrucciones de reglas y los detalles de las reglas que aparecen a continuación describen las capacidades y los requisitos de anidación de cada categoría y regla.

El editor visual de reglas de la consola admite solamente un nivel de anidamiento para instrucciones de reglas. Por ejemplo, puede anidar muchos tipos de instrucciones dentro de una regla lógica AND o OR, pero no puede anidar otra regla AND o OR, ya que eso requiere un segundo nivel de anidación. Para implementar varios niveles de anidación, proporcione la definición de la regla en JSON, ya sea a través del editor de reglas de JSON de la consola o a través de las API.

Temas

- Especificación y manejo de componentes de solicitudes web

- Instrucciones de restricción de acceso
- Instrucciones que hacen referencia a un conjunto o grupo de reglas

Especificación y manejo de componentes de solicitudes web

En esta sección se describen los ajustes que se pueden especificar en las sentencias de reglas que inspeccionan un componente de la solicitud web. Para obtener información sobre el uso, consulte las instrucciones de reglas individuales en instrucciones de coincidencia.

Un subconjunto de estos componentes de solicitudes web también se puede usar en reglas basadas en tasas, como claves de agregación de solicitudes personalizadas. Para obtener más información, consulte Opciones y claves de agregación de reglas basadas en tasas.

Para la configuración del componente de solicitud, especifique el tipo de componente en sí y cualquier opción adicional, en función del tipo de componente. Por ejemplo, al inspeccionar un tipo de componente que contiene texto, puede aplicarle transformaciones de texto antes de inspeccionarlo.

> **Note**
>
> A menos que se indique lo contrario, si una solicitud web no tiene el componente de solicitud especificado en la declaración de la regla, se considera que AWS WAF la solicitud no cumple con los criterios de la regla.

Contenido

  - Parámetro de consulta único
  - Todos los parámetros de consulta
  - Cuerpo
  - Cuerpo JSON
- Dirección IP reenviada
- Opciones para inspeccionar pseudoencabezados HTTP/2
- Opciones de transformación de texto

Opciones de componentes de solicitudes

En esta sección, se describen los componentes de la solicitud web que puede especificar para su inspección. Especifique el componente solicitado para las instrucciones de regla estándar que buscan patrones en la solicitud web. Estos tipos de sentencias incluyen la coincidencia de cadenas, la coincidencia regex, la restricción de tamaño y las sentencias de ataque por inyección de código SQL. Para obtener información sobre cómo usar esta configuración de los componentes de la solicitud, consulte las instrucciones de reglas individuales en instrucciones de coincidencia.

A menos que se indique lo contrario, si una solicitud web no tiene el componente de solicitud especificado en la declaración de la regla, AWS WAF evalúa que la solicitud no cumple con los criterios de la regla.

> **Note**
>
> Especifique un único componente de solicitud para cada instrucción de regla que lo requiera. Para inspeccionar más de un componente de una solicitud, cree una instrucción de regla para cada componente.

La documentación de la AWS WAF consola y la API proporciona orientación sobre la configuración de los componentes de la solicitud en las siguientes ubicaciones:

- Generador de reglas en la consola: en la configuración de Instrucción para un tipo de regla normal, elija el componente que desee inspeccionar en el cuadro de diálogo Inspeccionar de la sección Solicitar componentes.
- Contenido de la instrucción de API: `FieldToMatch`

En el resto de esta sección, se describen las opciones de la parte de la solicitud web que hay que inspeccionar.

Temas

Método HTTP

Comprueba el método HTTP en la solicitud. El método HTTP indica el tipo de operación que la solicitud web pide que realice su recurso protegido, como por ejemplo `POST` o `GET`.

Encabezado único

Inspecciona un encabezado con un solo nombre en la solicitud.

Para esta opción, especifique el nombre del encabezado, por ejemplo, `User-Agent` o `Referer`. La cadena que coincide con el nombre no distingue entre mayúsculas y minúsculas.

Todos los encabezados

Inspecciona todos los encabezados de las solicitudes, incluidas las cookies. Puede aplicar un filtro para inspeccionar un subconjunto de todos los encabezados.

Para esta opción, debe proporcionar las siguientes especificaciones:

- Patrones de coincidencia: el filtro que se utilizará para obtener un subconjunto de encabezados para su inspección. AWS WAF busca estos patrones en las teclas de encabezados.

  La configuración de los patrones de coincidencia puede ser una de las siguientes:

  - Todos: haga coincidir todas las claves. Evalúe los criterios de inspección de las reglas para todos los encabezados.
  - Encabezados excluidos Inspeccione solo los encabezados cuyas claves no coincidan con ninguna de las cadenas que ha especificado aquí. La cadena que coincide con la clave no distingue entre mayúsculas y minúsculas.
  - Encabezados incluidos Inspeccione solo los encabezados que tengan una clave que coincida con una de las cadenas que ha especificado aquí. La cadena que coincide con la clave no distingue entre mayúsculas y minúsculas.
- Alcance de coincidencia: las partes de los encabezados que AWS WAF deben inspeccionarse según los criterios de inspección de la regla. Puede especificar Claves, Valores o Todos para inspeccionar tanto las claves como los valores para ver si coinciden.

  Todos no precisa una coincidencia en las claves y una coincidencia en los valores. Es necesario encontrar una coincidencia en las claves, en los valores o en ambos. Para exigir una coincidencia en las claves y los valores, utilice una instrucción lógica `AND` para combinar dos reglas de coincidencia, una que inspeccione las claves y otra que inspeccione los valores.
- Manejo de sobredimensionamiento: ¿cómo se AWS WAF deben gestionar las solicitudes que tienen datos de encabezado más grandes de lo que se AWS WAF puede inspeccionar? AWS WAF puede inspeccionar como máximo los primeros 8 KB (8.192 bytes) de los encabezados de las solicitudes y, como máximo, los primeros 200 encabezados. El contenido está disponible para su inspección AWS WAF hasta que se alcance el primer límite. Puede elegir continuar con la inspección u omitir la inspección y marcar la solicitud como coincidente o no con la regla. Para obtener más información acerca de la administración del contenido de tamaño excesivo, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF.

Orden de encabezados

Inspeccione una cadena que contenga la lista de los nombres de los encabezados de la solicitud, ordenados tal como aparecen en la solicitud web que se AWS WAF recibe para su inspección. AWS WAF genera la cadena y luego la usa como campo para hacer coincidir el componente en su inspección. AWS WAF separa los nombres de los encabezados de la cadena con dos puntos y sin añadir espacios, por ejemplo`host:user-agent:accept:authorization:referer`.

Para esta opción, debe proporcionar las siguientes especificaciones:

- Gestión del tamaño excesivo: ¿cómo se AWS WAF deben gestionar las solicitudes que tienen datos de encabezado más numerosos o más grandes de lo que se AWS WAF puede inspeccionar? AWS WAF puede inspeccionar como máximo los primeros 8 KB (8.192 bytes) de los encabezados de las solicitudes y, como máximo, los primeros 200 encabezados. El contenido está disponible para su inspección AWS WAF hasta que se alcance el primer límite. Puede elegir continuar con la inspección de los encabezados que estén disponibles, o bien omitir la inspección y marcar la solicitud como coincidente o no con la regla. Para obtener más información acerca de la administración del contenido de tamaño excesivo, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF.

Cookies

Inspecciona todas las cookies de solicitud. Puede aplicar un filtro para inspeccionar un subconjunto de todas las cookies.

Para esta opción, debe proporcionar las siguientes especificaciones:

- Patrones de coincidencia: el filtro que se utilizará para obtener un subconjunto de cookies para su inspección. AWS WAF busca estos patrones en las claves de las cookies.

  La configuración de los patrones de coincidencia puede ser una de las siguientes:

  - Todos: haga coincidir todas las claves. Evalúe los criterios de inspección de las reglas para todas las cookies.
  - Cookies excluidas: inspeccione solo las cookies cuyas claves no coincidan con ninguna de las cadenas que ha especificado aquí. La coincidencia de cadena con una clave distingue entre mayúsculas y minúsculas, y debe ser exacta.
  - Encabezados incluidos: inspeccione solo las cookies que tengan una clave que coincida con una de las cadenas que ha especificado aquí. La coincidencia de cadena con una clave distingue entre mayúsculas y minúsculas, y debe ser exacta.
- Alcance de coincidencia: las partes de las cookies que AWS WAF deben inspeccionarse según los criterios de inspección de la regla. Puede especificar Claves, Valores o Todos tanto para las claves como para los valores.

  Todos no precisa una coincidencia en las claves y una coincidencia en los valores. Es necesario encontrar una coincidencia en las claves, en los valores o en ambos. Para exigir una coincidencia

en las claves y los valores, utilice una instrucción lógica `AND` para combinar dos reglas de coincidencia, una que inspeccione las claves y otra que inspeccione los valores.

- Gestión de sobredimensionamiento: ¿cómo se AWS WAF deben gestionar las solicitudes que contienen datos de cookies más grandes de los que se AWS WAF pueden inspeccionar? AWS WAF puede inspeccionar como máximo los primeros 8 KB (8.192 bytes) de las cookies solicitadas y, como máximo, las primeras 200 cookies. El contenido está disponible para su inspección AWS WAF hasta que se alcance el primer límite. Puede elegir continuar con la inspección u omitir la inspección y marcar la solicitud como coincidente o no con la regla. Para obtener más información acerca de la administración del contenido de tamaño excesivo, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF.

Ruta de URI

Inspecciona la parte de una URL que identifica un recurso, por ejemplo, `/images/daily-ad.jpg`. Para obtener información, consulte Identificador uniforme de recursos (URI): sintaxis genérica.

Si no utilizas una transformación de texto con esta opción, AWS WAF no normaliza el URI y lo inspecciona exactamente como lo recibe del cliente en la solicitud. Para obtener información sobre transformaciones de texto, consulte Opciones de transformación de texto.

Huella digital JA3

Inspecciona la huella digital JA3 de la solicitud.

> **Note**
>
> La inspección de huellas dactilares JA3 solo está disponible para CloudFront las distribuciones de Amazon y los balanceadores de carga de aplicaciones.

La huella digital JA3 es un hash de 32 caracteres derivado del saludo del cliente TLS de una solicitud entrante. Esta huella digital sirve como identificador único para la configuración de TLS del cliente. AWS WAF calcula y registra esta huella digital para cada solicitud que contenga suficiente información de TLS Client Hello para el cálculo. Casi todas las solicitudes web incluyen esta información.

Cómo obtener la huella digital JA3 para un cliente

Puede obtener la huella digital JA3 para las solicitudes de un cliente en los registros de la ACL web. Si AWS WAF es capaz de calcular la huella digital, la incluye en los registros. Para obtener información acerca de los campos de registro, consulte Campos de registro.

Requisitos de las instrucciones de reglas

Puede inspeccionar la huella digital JA3 solo dentro de una instrucción de coincidencia de cadena que esté configurada para que coincida exactamente con la cadena que proporcione. Proporcione la cadena de huella digital JA3 de los registros de la especificación de la instrucción de coincidencia de cadena para que coincida con cualquier solicitud futura que tenga la misma configuración de TLS. Para obtener más información acerca de las instrucciones de reglas de coincidencia de cadena, consulte Instrucción de regla de coincidencia de cadenas.

Debe proporcionar un comportamiento alternativo para esta instrucción de regla. El comportamiento alternativo es el estado de coincidencia que deseas asignar AWS WAF a la solicitud web si AWS WAF no puedes calcular la huella digital JA3. Si opta por hacer coincidir, AWS WAF trata la solicitud web como coincidente con la instrucción de regla y aplica la acción de la regla a la solicitud. Si eliges no coincidir, considerará que la AWS WAF solicitud no coincide con la declaración de la regla.

Para usar esta opción de coincidencia, debe registrar su tráfico de ACL web. Para obtener más información, consulte Registro del tráfico de ACL AWS WAF web.

Cadena de consulta

Inspecciona la parte de la URL que aparece después de un carácter ?, si hay alguno.

> **Note**
>
> En instrucciones de coincidencia de scripting entre sitios, recomendamos elegir Todos los parámetros de consulta en vez de Cadena de consulta. Si selecciona Todos los parámetros de la consulta, se añaden 10 WCU al coste base.

Parámetro de consulta único

Inspecciona un único parámetro de consulta que haya definido como parte de la cadena de consulta. AWS WAF inspecciona el valor del parámetro que especifique.

Para esta opción, también se especifica un Argumento de consulta. Si la dirección URL es `www.xyz.com?UserName=abc&SalesRegion=seattle`, puede especificar `UserName` o

`SalesRegion` como argumento de la consulta. La longitud máxima del nombre del argumento es de 30 caracteres. El nombre no distingue entre mayúsculas y minúsculas, por lo que si especifica `UserName`, AWS WAF busca coincidencias con todas las variantes de `UserName`, como `username` y `UsERName`.

Si la cadena de consulta contiene más de una instancia del argumento de consulta que ha especificado, AWS WAF inspecciona todos los valores para ver si coinciden con ellos mediante OR la lógica. Por ejemplo, en la dirección URL `www.xyz.com?SalesRegion=boston&SalesRegion=seattle`, AWS WAF evalúa el nombre que ha especificado con `boston` y `seattle`. Si alguna de las dos es una coincidencia, la inspección es una coincidencia.

Todos los parámetros de consulta

Inspecciona todos los parámetros de consulta de la solicitud. Es similar a la elección del componente de parámetro de consulta único, pero AWS WAF inspecciona los valores de todos los argumentos de la cadena de consulta. Por ejemplo, si la dirección URL es `www.xyz.com?UserName=abc&SalesRegion=seattle`, AWS WAF activa una coincidencia si el valor de `UserName` o `SalesRegion` coincide con los criterios de inspección.

Al elegir esta opción, se añaden 10 WCU al coste base.

Cuerpo

Inspecciona el cuerpo de la solicitud evaluada como texto sin formato. También puede evaluar el cuerpo como JSON utilizando el tipo de contenido JSON.

El cuerpo de la solicitud es la parte de la solicitud que sigue inmediatamente a los encabezados de solicitudes. Contiene los datos adicionales necesarios para la solicitud web, como los datos de un formulario.

- En la consola, seleccione Cuerpo en la opción Solicitud y, a continuación, Texto sin formato en Tipo de contenido.
- En la API, en la especificación `FieldToMatch` de la regla, especifique `Body` para inspeccionar el cuerpo de la solicitud como texto sin formato.

Para Application Load Balancer y AWS AppSync, AWS WAF puede inspeccionar los primeros 8 KB del cuerpo de una solicitud. Para CloudFront API Gateway, Amazon Cognito, App Runner y Verified Access, de forma predeterminada, AWS WAF pueden inspeccionar los primeros 16 KB y

usted puede aumentar el límite hasta 64 KB en su configuración de ACL web. Para obtener más información, consulte Gestión de los límites de tamaño de la inspección corporal.

Debe especificar la gestión del sobredimensionamiento para este tipo de componente. El manejo de sobredimensionamiento define la forma en AWS WAF que se gestionan las solicitudes que tienen un volumen de datos mayor del que se AWS WAF puede inspeccionar. Puede elegir continuar con la inspección u omitir la inspección y marcar la solicitud como coincidente o no con la regla. Para obtener más información acerca de la administración del contenido de tamaño excesivo, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF.

También puede evaluar el cuerpo como JSON analizado. Para obtener información sobre esto, consulte la sección siguiente.

Cuerpo JSON

Inspecciona el cuerpo de la solicitud, evaluado como JSON. También puede evaluar el cuerpo como texto sin formato.

El cuerpo de la solicitud es la parte de la solicitud que sigue inmediatamente a los encabezados de solicitudes. Contiene los datos adicionales necesarios para la solicitud web, como los datos de un formulario.

- En la consola, se selecciona en la Opción de solicitud Cuerpo, seleccionando la opción Tipo de contenido JSON.
- En la API, en la especificación `FieldToMatch` de la regla, especifique `JsonBody`.

Para Application Load Balancer y AWS AppSync, AWS WAF puede inspeccionar los primeros 8 KB del cuerpo de una solicitud. Para CloudFront API Gateway, Amazon Cognito, App Runner y Verified Access, de forma predeterminada, AWS WAF pueden inspeccionar los primeros 16 KB y usted puede aumentar el límite hasta 64 KB en su configuración de ACL web. Para obtener más información, consulte Gestión de los límites de tamaño de la inspección corporal.

Debe especificar la gestión del sobredimensionamiento para este tipo de componente. El manejo de sobredimensionamiento define la forma en AWS WAF que se gestionan las solicitudes que tienen un volumen de datos mayor del que se AWS WAF puede inspeccionar. Puede elegir continuar con la inspección u omitir la inspección y marcar la solicitud como coincidente o no con la regla. Para obtener más información acerca de la administración del contenido de tamaño excesivo, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF.

Cuando AWS WAF inspecciona el cuerpo de la solicitud web como JSON analizado, analiza y extrae los elementos del JSON e inspecciona las partes que tú indiques utilizando los criterios de la sentencia de coincidencia de la regla.

Al elegir esta opción, se duplica el coste base de las WCU de la instrucción de coincidencia. Por ejemplo, si el coste base de la instrucción de coincidencia es de 5 WCU sin análisis de JSON, el uso del análisis de JSON duplica el coste hasta 10 WCU.

Con esta opción, AWS WAF ejecuta dos patrones de coincidencia con el cuerpo de la solicitud web. La salida del primer patrón de coincidencia se utiliza como entrada para el segundo patrón de coincidencia:

1. AWS WAF analiza y extrae el contenido de JSON e identifica los elementos que se van a inspeccionar. Para ello, AWS WAF utiliza los criterios que proporciones en la especificación del cuerpo JSON de la regla.
2. AWS WAF aplica cualquier transformación de texto a los elementos extraídos y, a continuación, compara el conjunto de elementos JSON resultante con los criterios de coincidencia de la declaración de la regla. Si alguno de los elementos coincide, la solicitud web coincide con la regla.

Debe especificar los siguientes criterios AWS WAF para utilizarlos en el primer paso de coincidencia de patrones, a fin de identificar los elementos JSON que se van a inspeccionar:

- Comportamiento alternativo del análisis del cuerpo: qué debe hacer AWS WAF si no analiza completamente el cuerpo JSON. Las opciones son las siguientes:
  - Ninguno (comportamiento predeterminado): AWS WAF evalúa el contenido solo hasta el punto en que se ha detectado un error de análisis.
  - Evaluar como cadena: inspecciona el cuerpo como texto sin formato. AWS WAF aplica las transformaciones de texto y los criterios de inspección que ha definido para la inspección de JSON a la cadena de texto principal.
  - Coincidencia: considera que la solicitud web coincide con la declaración de la regla. AWS WAF aplica la acción de la regla a la solicitud.
  - Sin coincidencia: trate la solicitud web como no coincidente con la instrucción de regla.

  AWS WAF hace todo lo posible para analizar todo el cuerpo del JSON, pero es posible que se vea obligado a detenerlo por motivos como caracteres no válidos, claves duplicadas, truncamiento o cualquier contenido cuyo nodo raíz no sea un objeto o una matriz.

AWS WAF analiza el JSON de los siguientes ejemplos como dos pares clave y valor válidos:

- Falta de coma: `{"key1":"value1""key2":"value2"}`
- Falta de dos puntos: `{"key1":"value1","key2""value2"}`
- Dos puntos adicionales: `{"key1"::"value1","key2""value2"}`

- Ámbito de coincidencia de JSON: los tipos de elementos del JSON que AWS WAF se deben inspeccionar. Puede especificar Claves, Valores o Todos tanto para las claves como para los valores.

  Todos no precisa una coincidencia en las claves y una coincidencia en los valores. Es necesario encontrar una coincidencia en las claves, en los valores o en ambos. Para exigir una coincidencia en las claves y los valores, utilice una instrucción lógica `AND` para combinar dos reglas de coincidencia, una que inspeccione las claves y otra que inspeccione los valores.

- Contenido que se va a inspeccionar: los elementos del JSON analizado y extraído que deseas AWS WAF inspeccionar.

  Debe especificar uno de los siguientes:

  - Contenido completo de JSON: evalúa todos los elementos de la JSON analizado.
  - Solo elementos incluidos: evalúa solo los elementos de la JSON que coincidan con los criterios de JSON Pointer que proporcione. Para obtener información sobre la sintaxis del puntero JSON, consulte la documentación del Grupo de Trabajo de Ingeniería de Internet (IETF) sobre notación de JavaScript objetos (JSON) Pointer.

    No utilice esta opción para incluir todas las rutas de JSON. En su lugar, usa contenido JSON completo.

    Por ejemplo, en la consola, puede proporcionar lo siguiente:

    ```
    /dogs/0/name
    /dogs/1/name
    ```

    En la API o la CLI, puede proporcionar lo siguiente:

    ```
    "IncludedPaths": ["/dogs/0/name", "/dogs/1/name"]
    ```

Ejemplo de escenario de inspección del cuerpo JSON

Si la configuración de los elementos incluidos es `/a/b`, entonces, para el siguiente cuerpo JSON:

```
{
  "a":{
    "c":"d",
    "b":{
      "e":{
        "f":"g"
      }
    }
  }
}
```

En la siguiente lista se describe lo que AWS WAF se evaluaría para cada configuración del ámbito de coincidencia. La clave `b`, que forma parte de la ruta de elementos incluidos, no se evalúa.

- Para un alcance de coincidencia establecido en todos: `e`, `f`, y `g`.
- Para un ámbito de coincidencia establecido para las claves: `e` y `f`.
- Para un alcance de coincidencia establecido en valores: `g`.

Dirección IP reenviada

Esta sección se aplica a las instrucciones de reglas que utilizan la dirección IP de una solicitud web. De forma predeterminada, AWS WAF utiliza la dirección IP del origen de la solicitud web. Si el tráfico pasa por uno o más proxies o equilibradores de carga, el origen de la solicitud web contiende la dirección del último proxy y no la dirección de origen del cliente. En este caso, la dirección del cliente originario normalmente se reenvía en otro encabezado HTTP. Este encabezado suele ser `X-Forwarded-For` (XFF), pero puede ser diferente.

Instrucciones de reglas que usan direcciones IP

Las instrucciones de reglas que utilizan direcciones IP son las siguientes:

- Coincidencia de conjuntos de IP: inspecciona la dirección IP para ver si coincide con las direcciones definidas en un conjunto de IP.
- Coincidencia geográfica: utiliza la dirección IP para determinar el país y la región de origen, y compara el país de origen con una lista de países.
- Instrucción de regla basada en frecuencia: puede agregar las solicitudes por sus direcciones IP para garantizar que ninguna dirección IP individual envíe solicitudes a una tasa demasiado alta.

Puede utilizar la agregación de direcciones IP por sí sola o en combinación con otras claves de agregación.

Puedes AWS WAF indicarle que utilices una dirección IP reenviada para cualquiera de estas instrucciones de regla, ya sea desde el `X-Forwarded-For` encabezado o desde otro encabezado HTTP, en lugar de utilizar el origen de la solicitud web. Para obtener más información sobre cómo proporcionar las especificaciones, consulte la guía para cada tipo de instrucción de regla individual.

> **Note**
>
> Si el encabezado que especificas no está presente en la solicitud, AWS WAF no se aplica en absoluto la regla a la solicitud web.

Comportamiento alternativo

Cuando utilizas la dirección IP reenviada, indicas el estado de coincidencia AWS WAF que deseas asignar a la solicitud web si la solicitud no tiene una dirección IP válida en la posición especificada:

- COINCIDIR: considera que la solicitud web coincide con el enunciado de la regla. AWS WAF aplica la acción de la regla a la solicitud.
- SIN COINCIDENCIA: trate la solicitud web como no coincidente con la instrucción de regla.

Direcciones IP utilizadas en AWS WAF Bot Control

El grupo de reglas gestionado por Bot Control verifica los bots mediante las direcciones IP de AWS WAF. Si utiliza el control de bots y ha verificado bots enrutados a través de un proxy o un equilibrador de carga, debe permitirlos de forma explícita mediante una regla personalizada. Por ejemplo, puede configurar una regla de coincidencia de conjuntos de IP personalizada que utilice las direcciones IP reenviadas para detectar y admitir sus bots verificados. Puede usar la regla para personalizar la administración de los bots de varias maneras. Para obtener más información y ejemplos, consulte AWS WAF Control de bots.

Consideraciones generales sobre el uso de direcciones IP reenviadas

Antes de utilizar una dirección IP reenviada, tenga en cuenta las siguientes advertencias generales:

- Los proxies pueden modificar un encabezado a lo largo del proceso y los proxies pueden gestionar el encabezado de diferentes maneras.

- Los atacantes pueden alterar el contenido del encabezado en un intento de eludir las inspecciones de AWS WAF .
- La dirección IP incluida en el encabezado puede tener un formato incorrecto o no ser válida.
- Es posible que el encabezado que especifique no esté presente en absoluto en una solicitud.

Consideraciones sobre el uso de direcciones IP reenviadas con AWS WAF

En la siguiente lista se describen los requisitos y las advertencias para el uso de direcciones IP reenviadas en AWS WAF:

- Para cualquier regla individual, puede especificar un encabezado para la dirección IP reenviada. La especificación del encabezado no distingue entre mayúsculas y minúsculas.
- En el caso de las instrucciones de reglas basadas en tasas, las instrucciones de alcance anidadas no heredan la configuración de IP reenviada. Especifique la configuración de cada instrucción que utilice una dirección IP reenviada.
- Para las reglas de concordancia geográfica y basadas en tasas, AWS WAF usa la primera dirección del encabezado. Por ejemplo, si un encabezado contiene usos `10.1.1.1, 127.0.0.0, 10.10.10.10` AWS WAF `10.1.1.1`
- En el caso de la coincidencia de conjuntos de IP, debe indicar si debe coincidir con la primera, la última o con cualquier otra dirección del encabezado. Si especifica alguno, AWS WAF inspecciona todas las direcciones del encabezado para ver si coinciden, hasta un máximo de 10 direcciones. Si el encabezado contiene más de 10 direcciones, AWS WAF inspecciona las 10 últimas.
- Los encabezados que contienen varias direcciones deben usar una coma de separación entre las direcciones. Si una solicitud utiliza un separador que no sea una coma, AWS WAF considera que las direcciones IP del encabezado tienen un formato incorrecto.
- Si las direcciones IP incluidas en el encabezado tienen un formato incorrecto o no son válidas, AWS WAF indica que la solicitud web coincide con la regla o no coincide, de acuerdo con el comportamiento alternativo que especifique en la configuración de IP reenviada.
- Si el encabezado que especificas no está presente en una solicitud, AWS WAF no se aplica en absoluto la regla a la solicitud. Esto significa que AWS WAF no aplica la acción de la regla ni el comportamiento alternativo.
- Una instrucción de regla que utilice un encabezado IP reenviado como dirección IP no utilizará la dirección IP indicada por el origen de la solicitud web.

Prácticas recomendadas para usar direcciones IP reenviadas con AWS WAF

Al utilizar direcciones IP reenviadas, siga las siguientes prácticas recomendadas:

- Considera detenidamente todos los estados posibles de los encabezados de sus solicitudes antes de habilitar la configuración de IP reenviada. Es posible que tenga que usar más de una regla para obtener el comportamiento que desea.
- Para inspeccionar varios encabezados IP reenviados o para inspeccionar el origen de una solicitud web y un encabezado IP reenviado, use una regla para cada origen de direcciones IP.
- Para bloquear las solicitudes web que tengan un encabezado no válido, defina la acción de regla para bloquear y establezca el comportamiento alternativo para que coincida con la configuración de IP reenviada.

Ejemplo de JSON para direcciones IP reenviadas

La siguiente instrucción de coincidencia geográfica solo coincide si el encabezado `X-Forwarded-For` contiene una IP cuyo país de origen es US:

```
{
  "Name": "XFFTestGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestGeo"
  },
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ],
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

La siguiente regla basada en tasas agrega las solicitudes en función de la primera IP del encabezado `X-Forwarded-For`. La regla solo cuenta las solicitudes que coinciden con la instrucción de coincidencia geográfica anidada y solo bloquea las solicitudes que coinciden con la instrucción de coincidencia geográfica. La instrucción de coincidencia geográfica anidada también utiliza el encabezado `X-Forwarded-For` para determinar si la dirección IP indica un país de origen de US. Si es así, o si el encabezado está presente pero tiene un formato incorrecto, la instrucción de coincidencia geográfica devuelve una coincidencia.

```
{
  "Name": "XFFTestRateGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestRateGeo"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": "100",
      "AggregateKeyType": "FORWARDED_IP",
      "ScopeDownStatement": {
        "GeoMatchStatement": {
          "CountryCodes": [
            "US"
          ],
          "ForwardedIPConfig": {
            "HeaderName": "x-forwarded-for",
            "FallbackBehavior": "MATCH"
          }
        }
      },
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

Opciones para inspeccionar pseudoencabezados HTTP/2

AWS Los recursos protegidos que admiten el tráfico HTTP/2 no reenvían los pseudoencabezados de HTTP/2 AWS WAF para su inspección, pero proporcionan el contenido de los pseudoencabezados en los componentes de las solicitudes web que se inspeccionan. AWS WAF

Puede utilizarlos AWS WAF para inspeccionar únicamente los pseudoencabezados que se muestran en la siguiente tabla.

El contenido de los pseudoencabezados de HTTP/2 está asignado a los componentes de las solicitudes web

Pseudoencabezado de HTTP/2	Componente de solicitud web que inspeccionar	Documentación
`:method`	Método HTTP	Método HTTP
`:authority`	Encabezado `Host`	Encabezado único Todos los encabezados
Ruta de URI `:path`	Ruta de URI	Ruta de URI
Consulta de `:path`	Cadena de consulta	Cadena de consulta Parámetro de consulta único Todos los parámetros de consulta

Opciones de transformación de texto

En las instrucciones que buscan patrones o establecen restricciones, puede proporcionar transformaciones AWS WAF para que se apliquen antes de inspeccionar la solicitud. Una transformación reformatea una solicitud web para eliminar parte del formato inusual que los atacantes utilizan con el objetivo de eludir AWS WAF.

Si lo utiliza con la selección de componentes de la solicitud del cuerpo JSON, AWS WAF aplica las transformaciones después de analizar y extraer los elementos de la JSON para inspeccionarlos. Para obtener más información, consulte Cuerpo JSON.

Si proporciona más de una transformación, también establece la orden para que AWS WAF las aplique.

Unidad de capacidad de escritura (WCU): cada transformación de texto equivale a 10 WCU.

La documentación de la AWS WAF consola y la API también proporciona orientación sobre estos ajustes en las siguientes ubicaciones:

- Generador de reglas en la consola: Transformación de texto. Esta opción está disponible cuando se utilizan componentes de solicitud.
- Contenido de la instrucción de API: `TextTransformations`

Opciones para transformaciones de texto

Cada lista de transformaciones muestra las especificaciones de la consola y la API seguidas de una descripción.

Base64 decode – `BASE64_DECODE`

AWS WAF decodifica una cadena codificada en Base64.

Base64 decode extension – `BASE64_DECODE_EXT`

AWS WAF decodifica una cadena codificada en Base64, pero usa una implementación flexible que ignora los caracteres que no son válidos.

Command line – `CMD_LINE`

Esta opción mitiga las situaciones en las que los atacantes podrían estar inyectando un comando de línea de comandos del sistema operativo y utilizando un formato inusual para disfrazar una parte o la totalidad del comando.

Utilice esta opción para realizar las siguientes transformaciones:

- Eliminar los siguientes caracteres: `\ " ' ^`
- Eliminar los espacios delante de los siguientes caracteres: `/ (`
- Sustituir los siguientes caracteres por un espacio: `, ;`

- Sustituir varios espacios por un espacio
- Convertir letras mayúsculas, `A-Z`, a minúsculas, `a-z`

Compress whitespace – `COMPRESS_WHITE_SPACE`

AWS WAF comprime los espacios en blanco sustituyendo varios espacios por un espacio y sustituyendo los siguientes caracteres por un carácter de espacio (ASCII 32):

- Avance de página (ASCII 12)
- Pestaña (ASCII 9)
- Nueva línea (ASCII 10)
- Retorno de carro (ASCII 13)
- Pestaña vertical (ASCII 11)
- Espacio duro (ASCII 160)

CSS decode – `CSS_DECODE`

AWS WAF decodifica los caracteres codificados mediante las reglas de escape de CSS 2.x. `syndata.html#characters` Esta función utiliza hasta dos bytes en el proceso de decodificación, por lo que puede ayudar a descubrir caracteres ASCII que se codificaron en CSS y que normalmente no se codificarían. También es útil para contrarrestar la evasión, que es una combinación de una barra invertida y caracteres no hexadecimales. Por ejemplo, `ja\vascript` para `javascript`.

Escape sequences decode – `ESCAPE_SEQ_DECODE`

AWS WAF decodifica las siguientes secuencias de escape ANSI C:`\a`,,`\b`,`\f`,`\n`,`\r`,`\t`,, `\v\\`, `\xHH` (hexadecimal) `\? \'\"`, `\0000` (octal). Las codificaciones que no son válidas permanecen en la salida.

Hex decode – `HEX_DECODE`

AWS WAF decodifica una cadena de caracteres hexadecimales en un binario.

HTML entity decode – `HTML_ENTITY_DECODE`

AWS WAF reemplaza los caracteres que se representan en formato hexadecimal `&#xhhhh;` o decimal por `&#nnnn;` los caracteres correspondientes.

AWS WAF reemplaza los siguientes caracteres codificados en HTML por caracteres no codificados. Esta lista utiliza la codificación HTML en minúsculas, pero el manejo no distingue entre mayúsculas y minúsculas, por ejemplo, y se tratan de la misma manera. `&Qu0t; "`

Carácter codificado en HTML	sustituido por…
"	"
&	&
<	<
>	>
o	espacio de no separación, 160 decimales
\n, decimal 10
	\t, decimal 9
{ o {	{
|,	o		|
} o }	}
!	!
#	#
$	$
&percent; o %	%
'	\
(	(
)	)
* o *	*
+	+
,	,

Carácter codificado en HTML	sustituido por…
`.`	`.`
`/`	`/`
`:`	`:`
`;`	`;`
`=`	`=`
`?`	`?`
`˜` o `˜`	`~`
`−`	`-`
`[` o `[`	`[`
`\`	`\\`
`]` o `]`	`]`
`&hat;`	`^`
`_` o `&underbar;`	`_`
`` o ```	`` ` ``

JS decode – `JS_DECODE`

AWS WAF decodifica secuencias de escape JavaScript . Si un código `\uHHHH` está en el rango del código ASCII de ancho completo de `FF01-FF5E`, el byte superior se utiliza para detectar y ajustar el byte inferior. Si no, solo se utiliza el byte inferior y el byte superior se pone en cero, lo que provoca una posible pérdida de información.

Lowercase – `LOWERCASE`

AWS WAF convierte letras mayúsculas (A-Z) en minúsculas (a-z).

MD5 – `MD5`

AWS WAF calcula un hash MD5 a partir de los datos de la entrada. El hash calculado está en forma binaria sin procesar.

None – `NONE`

AWS WAF inspecciona la solicitud web tal como se recibió, sin ninguna transformación de texto.

Normalize path – `NORMALIZE_PATH`

AWS WAF normaliza la cadena de entrada eliminando las barras diagonales múltiples, las autorreferencias de los directorios y las referencias inversas de los directorios que no estén al principio de la entrada.

Normalize path Windows – `NORMALIZE_PATH_WIN`

AWS WAF convierte los caracteres de barra invertida en barras diagonales y, a continuación, procesa la cadena resultante mediante la transformación. `NORMALIZE_PATH`

Remove nulls – `REMOVE_NULLS`

AWS WAF elimina todos los `NULL` bytes de la entrada.

Replace comments – `REPLACE_COMMENTS`

AWS WAF reemplaza cada aparición de un comentario de estilo C (/*... */) por un solo espacio. No comprime varias repeticiones consecutivas. Sustituye los comentarios no finalizados terminados por un espacio (ASCII 0x20). No cambia la finalización independiente de un comentario (*/).

Replace nulls – `REPLACE_NULLS`

AWS WAF reemplaza cada `NULL` byte de la entrada por el carácter de espacio (ASCII 0x20).

SQL hex decode – `SQL_HEX_DECODE`

AWS WAF decodifica los datos hexadecimales de SQL. Por ejemplo, AWS WAF decodifica (`0x414243`) en (). `ABC`

URL decode – `URL_DECODE`

AWS WAF decodifica un valor codificado en una URL.

URL decode Unicode – `URL_DECODE_UNI`

Como `URL_DECODE`, pero compatible con la codificación de `%u` específica de Microsoft. Si el código está en el rango `FF01-FF5E` del código ASCII de ancho completo, el byte superior se

utiliza para detectar y ajustar el byte inferior. De lo contrario, solo se utiliza el byte inferior y el byte superior se pone en cero.

UTF8 to Unicode – `UTF8_TO_UNICODE`

AWS WAF convierte todas las secuencias de caracteres UTF-8 a Unicode. Esto ayuda a normalizar la entrada y minimiza los falsos positivos y los falsos negativos en idiomas distintos del inglés.

Instrucciones de restricción de acceso

Una instrucción de restricción de acceso es una instrucción de regla que se puede anidar que se añade a una instrucción de un grupo de reglas administrado o una instrucción basada en tasas para reducir el conjunto de solicitudes que evalúa la regla contenedora. La regla contenedora solo evalúa las solicitudes que coincidan primero con la instrucción de restricción de acceso.

- Declaración de grupo de reglas administrado: si agrega una declaración de alcance reducido a una declaración de grupo de reglas administrado, AWS WAF evalúa cualquier solicitud que no coincida con la declaración de alcance reducido como si no coincidiera con el grupo de reglas. Las solicitudes solo se evalúan por el grupo de reglas si coinciden con la instrucción de alcance descendente. En el caso de los grupos de reglas administrados cuyos precios se basan en la cantidad de solicitudes evaluadas, las instrucciones de restricción de acceso pueden ayudar a contener los costos.

  Para obtener más información acerca de las instrucciones sobre los grupos de reglas administrados, consulte Instrucción de grupo de reglas administrado.
- Instrucción de regla basada en tasas: una instrucción de regla basada en tasas sin una instrucción de restricción de acceso limita todas las solicitudes que evalúa la regla. Si solo quiere controlar la tasa para una categoría específica de solicitudes, agregue una instrucción de restricción de acceso a la regla basada en tasas. Por ejemplo, para rastrear y controlar únicamente la tasa de solicitudes de un área geográfica específica, puede especificar esa área geográfica en una instrucción de coincidencia geográfica y agregarla a su regla basada en tasas como instrucción de restricción de acceso.

  Para obtener más información acerca de las instrucciones de las reglas basadas en tasas, consulte Instrucción de regla basada en frecuencia.

Puede usar cualquier regla anidable en una instrucción de restricción de acceso. Para ver las instrucciones disponibles, consulte instrucciones de coincidencia y instrucciones de reglas lógicas. Las WCU de una instrucción de restricción de acceso son las WCU necesarias para la instrucción de regla que defina en ella. No se aplica ningún coste adicional por el uso de una instrucción de restricción de acceso.

Puede configurar una instrucción de restricción de acceso de la misma manera que lo hace cuando usa la instrucción en una regla normal. Por ejemplo, puede aplicar transformaciones de texto a un componente de una solicitud web que esté inspeccionando y puede especificar una dirección IP reenviada para usarla como dirección IP. Estas configuraciones se aplican solo a la instrucción de restricción de acceso y no las hereda el grupo de reglas administrado que las contiene ni la instrucción de regla basada en tasas.

Por ejemplo, si aplica transformaciones de texto a una cadena de consulta de la instrucción de restricción de acceso, la instrucción de restricción de acceso inspecciona la cadena de consulta después de aplicar las transformaciones. Si la solicitud coincide con los criterios de la instrucción de restricción de acceso, AWS WAF pasa la solicitud web a la regla contenedora en su estado original, sin las transformaciones de la instrucción de restricción de acceso. La regla que contiene la instrucción de restricción de acceso puede aplicar sus propias transformaciones de texto, pero no hereda ninguna de la instrucción de restricción de acceso.

No puede usar una instrucción de restricción de acceso para especificar ninguna configuración de inspección de solicitudes para la instrucción de la regla contenedora. No puede usar una instrucción de restricción de acceso como preprocesador de solicitudes web para la instrucción de regla contenedora. La única función de una instrucción de regla contenedora es determinar qué solicitudes se pasan a la instrucción de regla contenedora para su inspección.

Instrucciones que hacen referencia a un conjunto o grupo de reglas

Algunas reglas utilizan entidades que son reutilizables y que usted o un AWS Marketplace vendedor administran fuera de las ACL web. AWS Cuando se actualiza la entidad reutilizable, AWS WAF propaga la actualización a la regla. Por ejemplo, si utilizas un grupo de reglas AWS administradas en una ACL web, al AWS actualizar el grupo de reglas, AWS propaga el cambio a tu ACL web para actualizar su comportamiento. Si utiliza una sentencia de conjunto de direcciones IP en una regla, al actualizar el conjunto, se AWS WAF propaga el cambio a todas las reglas que hacen referencia a ella, de modo que cualquier ACL web que utilice esas reglas se conservará up-to-date junto con los cambios.

Las siguientes son las entidades reutilizables que se pueden utilizar en una instrucción de regla.

- Conjuntos de IP: cree y administre sus propios conjuntos de IP. En la consola, puede acceder a ellos desde el panel de navegación. Para obtener más información acerca de la administración de conjuntos de IP, consulte Conjuntos de IP y conjuntos de patrones de expresiones regulares en AWS WAF.
- Conjuntos de coincidencias: cree y administre sus propios conjuntos de coincidencias de regex. En la consola, puede acceder a ellos desde el panel de navegación. Para obtener más información acerca de la administración de conjuntos de patrones de regex, consulte Conjuntos de IP y conjuntos de patrones de expresiones regulares en AWS WAF.
- AWS Grupos de reglas de reglas administradas: AWS administra estos grupos de reglas. En la consola, podrá usarlos al agregar un grupo de reglas administrado a la ACL web. Para obtener más información al respecto, consulte AWS Lista de grupos de reglas de Managed Rules.
- AWS Marketplace grupos de reglas gestionados: AWS Marketplace los vendedores administran estos grupos de reglas y puedes suscribirte a ellos para usarlos. Para administrar las suscripciones, en el panel de navegación de la consola, elija AWS Marketplace. Los grupos de reglas AWS Marketplace administrados se muestran cuando agrega un grupo de reglas administrado a su ACL web. En el caso de los grupos de reglas a los que aún no se ha suscrito, también encontrará un enlace AWS Marketplace en esa página. Para obtener más información sobre los grupos de reglas gestionados por el AWS Marketplace vendedor, consultaAWS Marketplace grupos de reglas gestionados.
- Sus propios grupos de reglas: puede administrar sus propios grupos de reglas, normalmente cuando necesita algún comportamiento que no está disponible a través de los grupos de reglas administrados. En la consola, puede acceder a ellos desde el panel de navegación. Para obtener más información, consulte Administrar sus propios grupos de reglas.

Eliminación de un conjunto o un grupo de reglas al que se hace referencia

Al eliminar una entidad a la que se hace referencia, AWS WAF comprueba si se está utilizando actualmente en una ACL web. Si AWS WAF descubre que está en uso, te avisa. AWS WAF casi siempre es capaz de determinar si una ACL web está haciendo referencia a una entidad. Sin embargo, es posible que en algunas ocasiones no consiga hacerlo. Si tiene que asegurarse de que la entidad que quiere eliminar no se está utilizando, compruebe las ACL web antes de eliminarla.

instrucciones de coincidencia

Las instrucciones de coincidencia comparan la solicitud web o su origen con las condiciones que proporcione. Para muchas declaraciones de este tipo, AWS WAF compara un componente específico de la solicitud para encontrar contenido coincidente.

Las instrucciones de coincidencia se pueden anidar. Puede anidar cualquiera de estas instrucciones dentro de las instrucciones de reglas lógicas y puede utilizarlas en instrucciones de restricción de acceso. Para obtener información sobre las instrucciones de reglas lógicas, consulte instrucciones de reglas lógicas. Para obtener información sobre las instrucciones de restricción de acceso, consulte Instrucciones de restricción de acceso.

Esta tabla describe las instrucciones de coincidencia regulares que puede agregar a una regla y proporciona algunas pautas para calcular el uso de unidades de capacidad de ACL web (WCU) para cada una. Para obtener información acerca de las WCU, consulte AWS WAF unidades de capacidad ACL web (WCU).

instrucción de coincidencia	Descripción	WCU
Coincidencia geográfica	Inspecciona el país de origen de la solicitud y aplica etiquetas para el país y la región de origen.	1
Coincidencia de conjuntos de IP	Inspecciona la solicitud con un conjunto de direcciones IP y rangos de direcciones.	1 para la mayoría de los casos. Si configura la instrucción para usar un encabezado con direcciones IP reenviadas y especifica una posición en el encabezado de Any, aumente las WCU en 4.
Instrucción de regla de coincidencia de etiquetas	Inspecciona la solicitud en busca de etiquetas que hayan sido agregadas por otras reglas de la misma ACL web.	1

instrucción de coincidencia	Descripción	WCU
Instrucción de regla de coincidencia de expresiones regulares	Compara un patrón de regex con un componente de solicitud especificado.	3, como coste base. Si utiliza el componente de solicitud Todos los parámetros de consulta, añada 10 WCU. Si utiliza el Cuerpo JSON del componente de la solicitud, duplique el coste base de las WCU. Para cada Transformación de texto que aplique, añada 10 WCU.
Conjunto de patrones de expresiones regex	Compara patrones de regex con un componente de solicitud especificado.	25 por conjunto de patrones, como coste base. Si utiliza el componente de solicitud Todos los parámetros de consulta, añada 10 WCU. Si utiliza el Cuerpo JSON del componente de la solicitud, duplique el coste base de las WCU. Para cada Transformación de texto que aplique, añada 10 WCU.

instrucción de coincidencia	Descripción	WCU
Restricción de tamaño	Comprueba restricciones de tamaño con un componente de solicitud especificado.	1, como coste base. Si utiliza el componente de solicitud Todos los parámetros de consulta, añada 10 WCU. Si utiliza el Cuerpo JSON del componente de la solicitud, duplique el coste base de las WCU. Para cada Transformación de texto que aplique, añada 10 WCU.
Ataque de inyección de código SQL	Inspecciona el código SQL malintencionado en un componente de solicitud especificado.	20, como coste base. Si utiliza el componente de solicitud Todos los parámetros de consulta, añada 10 WCU. Si utiliza el Cuerpo JSON del componente de la solicitud, duplique el coste base de las WCU. Para cada Transformación de texto que aplique, añada 10 WCU.

instrucción de coincidencia	Descripción	WCU
Coincidencia de cadenas	Compara una cadena con un componente de solicitud especificado.	El coste base depende del tipo de coincidencia de cadenas y oscila entre 1 y 10. Si utiliza el componente de solicitud Todos los parámetros de consulta, añada 10 WCU. Si utiliza el Cuerpo JSON del componente de la solicitud, duplique el coste base de las WCU. Para cada Transformación de texto que aplique, añada 10 WCU.
Ataque de scripting XSS	Inspecciona los ataques de scripting entre sitios en un componente de solicitud especificado.	40, como coste base. Si utiliza el componente de solicitud Todos los parámetros de consulta, añada 10 WCU. Si utiliza el Cuerpo JSON del componente de la solicitud, duplique el coste base de las WCU. Para cada Transformación de texto que aplique, añada 10 WCU.

Instrucción de regla de coincidencia geográfica

Utilice instrucciones de concordancia geográfica para administrar las solicitudes web en función del país y la región de origen. Una instrucción de concordancia geográfica agrega etiquetas a las solicitudes web que indican el país de origen y la región de origen. Añade estas etiquetas independientemente de si los criterios de la instrucción coinciden con los de la solicitud. Una instrucción de coincidencia geográfica también realiza una comparación con el país de origen de la solicitud.

¿Cómo usar la instrucción de coincidencia geográfica

Puede usar la instrucción de coincidencia geográfica para la coincidencia de países o regiones, de la siguiente manera:

- País: puede usar una regla de coincidencia geográfica por sí sola para gestionar las solicitudes en función únicamente de su país de origen. La instrucción de regla coincide con los códigos de país. También puede seguir una regla de coincidencia geográfica con una regla de coincidencia de etiquetas que coincida con la etiqueta del país de origen.
- Región: use una regla de coincidencia geográfica seguida de una regla de coincidencia de etiquetas para gestionar las solicitudes en función de su región de origen. No puede usar una regla de coincidencia geográfica por sí sola para hacer coincidir los códigos de región.

Para obtener información sobre el uso de las reglas de coincidencia de etiquetas, consulte Instrucción de regla de coincidencia de etiquetas y AWS WAF etiquetas en las solicitudes web.

Cómo funciona la instrucción de coincidencia geográfica

Con la declaración geo match, AWS WAF gestiona cada solicitud web de la siguiente manera:

1. Determina los códigos de país y región de la solicitud: AWS WAF determina el país y la región de una solicitud en función de su dirección IP. De forma predeterminada, AWS WAF utiliza la dirección IP del origen de la solicitud web. Puedes indicar AWS WAF que uses una dirección IP de un encabezado de solicitud alternativo, por ejemplo`X-Forwarded-For`, habilitando la configuración de IP reenviada en la configuración de la declaración de reglas.

   AWS WAF determina la ubicación de las solicitudes mediante bases de datos de MaxMind GeoIP. MaxMind informa de una precisión muy alta de sus datos a nivel de país, aunque la precisión varía según factores como el país y el tipo de IP. Para obtener más información MaxMind, consulte Geolocalización de MaxMind IP. Si cree que alguno de los datos de GeoIP es incorrecto, puede enviar una solicitud de corrección a Maxmind en MaxMind Correct GeoIP2 Data.

   AWS WAF utiliza los códigos de país y región alfa-2 de la norma 3166 de la Organización Internacional de Normalización (ISO). Puede encontrar los códigos en las siguientes ubicaciones:

   - En el sitio web de la ISO, puede buscar los códigos de los países en la Plataforma de navegación en línea (OBP) de la ISO.
   - En Wikipedia, los códigos de los países figuran en la ISO 3166-2.

Los códigos de región de un país aparecen en la URL `https://en.wikipedia.org/wiki/ISO_3166-2:<ISO country code>`. Por ejemplo, las regiones de los Estados Unidos están en la ISO 3166-2:US y, las de Ucrania, en la norma ISO 3166-2:UA.

2. Determina la etiqueta de país y la etiqueta de región que se van a agregar a la solicitud: las etiquetas indican si la instrucción de coincidencia geográfica utiliza la configuración de IP de origen o de IP reenviada.

   - ID de origen

     La etiqueta del país es `awswaf:clientip:geo:country:<ISO country code>`. Ejemplo para los Estados Unidos: `awswaf:clientip:geo:country:US`.

     La etiqueta de la región es `awswaf:clientip:geo:region:<ISO country code>-<ISO region code>`. Ejemplo para los Oregón, en Estados Unidos: `awswaf:clientip:geo:region:US-OR`.

   - IP reenviada

     La etiqueta del país es `awswaf:forwardedip:geo:country:<ISO country code>`. Ejemplo para los Estados Unidos: `awswaf:forwardedip:geo:country:US`.

     La etiqueta de la región es `awswaf:forwardedip:geo:region:<ISO country code>-<ISO region code>`. Ejemplo para los Oregón, en Estados Unidos: `awswaf:forwardedip:geo:region:US-OR`.

   Si el código de país o región no está disponible para la dirección IP especificada de una solicitud, AWS WAF utiliza `XX` en las etiquetas, en lugar del valor. Por ejemplo, la siguiente etiqueta es para la IP de un cliente cuyo código de país no está disponible: `awswaf:clientip:geo:country:XX` y la siguiente es para una IP reenviada cuyo país es Estados Unidos, pero cuyo código de región no está disponible: `awswaf:forwardedip:geo:region:US-XX`.

3. Evalúa el código de país de la solicitud según los criterios de la regla

La instrucción de coincidencia geográfica agrega etiquetas de país y región a todas las solicitudes que inspecciona, independientemente de si encuentra o no una coincidencia.

> **Note**
>
> AWS WAF añade cualquier etiqueta al final de la evaluación de la solicitud web de una regla. Por este motivo, cualquier coincidencia de etiquetas que utilice con las etiquetas de una instrucción de coincidencia geográfica debe definirse en una regla independiente de la regla que contiene la instrucción de coincidencia geográfica.

Si quiere inspeccionar solo los valores de las regiones, puede escribir una regla de coincidencia geográfica con la acción Count y con una sola coincidencia de códigos de país, seguida de una regla de coincidencia de etiquetas para las etiquetas de las regiones. Debe proporcionar un código de país para que la regla de coincidencia geográfica lo evalúe, incluso para este enfoque. Puede reducir el registro y las métricas de recuento especificando un país que muy probablemente no sea un origen de tráfico para su sitio.

CloudFront distribuciones y la función de restricción CloudFront geográfica

En el caso de CloudFront las distribuciones, si utilizas la función de restricción CloudFront geográfica, ten en cuenta que la función no reenvía las solicitudes bloqueadas a. AWS WAF Reenvía las solicitudes permitidas a AWS WAF. Si quieres bloquear las solicitudes en función de la zona geográfica y de otros criterios que puedas especificar AWS WAF, utiliza la declaración de concordancia AWS WAF geográfica y no utilices la función de restricción CloudFront geográfica.

Características de la instrucción de coincidencia geográfica

Se puede anidar: puede anidar este tipo de instrucción.

WCU: 1 WCU.

Configuración: esta instrucción utiliza la siguiente configuración:

- Códigos de país: conjunto de códigos de países que se pueden comparar para obtener una coincidencia geográfica. Deben ser códigos de país de dos caracteres, de los códigos ISO de país alfa-2 de la norma internacional ISO 3166, por ejemplo, `["US","CN"]`.
- (Opcional) Configuración de IP reenviada: de forma predeterminada, AWS WAF utiliza la dirección IP del origen de la solicitud web para determinar el país de origen. Como alternativa, puedes configurar la regla para que utilice una IP reenviada en un encabezado HTTP, como en `X-Forwarded-For` su lugar. AWS WAF usa la primera dirección IP del encabezado. Con esta configuración, también se especifica un comportamiento alternativo para aplicarlo a una solicitud web con una dirección IP con un formato incorrecto en el encabezado. El comportamiento

alternativo establece que el resultado de la solicitud coincide o no coincide. Para obtener más información, consulte Dirección IP reenviada.

Dónde encontrar esta instrucción de regla

- Generador de reglas en la consola: en Opción de la solicitud, elija Se origina desde un país de.
- API — GeoMatchStatement

Ejemplos

Puede utilizar la instrucción de coincidencia geográfica para administrar las solicitudes de países o regiones específicos. Por ejemplo, para bloquear determinados países, pero seguir permitiendo solicitudes de un conjunto específico de direcciones IP de uno de esos países, podría crear una regla con la acción establecida en Block y las siguientes instrucciones anidadas:

- AND instrucción
  - Instrucción de coincidencia geográfica en la que se enumeran los países que desea bloquear
  - NOT instrucción
    - Instrucción de conjuntos de IP que especifica las direcciones IP que desea permitir

O bien, si quiere bloquear algunas regiones de determinados países y, al mismo tiempo, permitir solicitudes de otras regiones de esos países, puede definir primero una regla de coincidencia geográfica con la acción establecida en Count. A continuación, defina una regla de coincidencia de etiquetas que coincida con las etiquetas de coincidencia geográfica agregadas y gestione las solicitudes según sea necesario.

El siguiente pseudocódigo describe un ejemplo de este enfoque:

1. Instrucción de coincidencia geográfica en la que se enumeran los países cuyas regiones quiere bloquear, pero con la acción configurada como Recuento. Esto etiqueta todas las solicitudes web, independientemente del estado de coincidencia, y también proporciona métricas de recuento de los países de interés.
2. Instrucción AND con acción de bloqueo
   - Instrucción de concordancia de etiquetas que especifica las etiquetas de los países que desea bloquear
   - NOT instrucción

- Instrucción de coincidencia de etiquetas que especifica las etiquetas de las regiones de los países por los que quiere permitir el paso

La siguiente lista de JSON muestra una implementación de las dos reglas descritas en el pseudocódigo anterior. Estas reglas bloquean todo el tráfico procedente de los Estados Unidos, excepto el tráfico procedente de Oregón y Washington. La instrucción de coincidencia geográfica agrega etiquetas de país y región a todas las solicitudes que inspecciona. La regla de coincidencia de etiquetas se ejecuta después de la regla de coincidencia geográfica, por lo que puede coincidir con las etiquetas de país y región que la regla de coincidencia geográfica acaba de agregar. La instrucción de coincidencia geográfica utiliza una dirección IP reenviada, por lo que la coincidencia de etiquetas también especifica las etiquetas de IP reenviadas.

```
{
   "Name": "geoMatchForLabels",
   "Priority": 10,
   "Statement": {
     "GeoMatchStatement": {
       "CountryCodes": [
         "US"
       ],
       "ForwardedIPConfig": {
           "HeaderName": "X-Forwarded-For",
           "FallbackBehavior": "MATCH"
       }
     }
   },
   "Action": {
     "Count": {}
   },
   "VisibilityConfig": {
     "SampledRequestsEnabled": true,
     "CloudWatchMetricsEnabled": true,
     "MetricName": "geoMatchForLabels"
   }
},
{
   "Name": "blockUSButNotOROrWA",
   "Priority": 11,
   "Statement": {
     "AndStatement": {
       "Statements": [
```

```
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:forwardedip:geo:country:US"
            }
          },
          {
            "NotStatement": {
              "Statement": {
                 "OrStatement": {
                   "Statements": [
                     {
                        "LabelMatchStatement": {
                          "Scope": "LABEL",
                          "Key": "awswaf:forwardedip:geo:region:US-OR"
                        }
                     },
                     {
                        "LabelMatchStatement": {
                          "Scope": "LABEL",
                          "Key": "awswaf:forwardedip:geo:region:US-WA"
                        }
                     }
                   ]
                 }
              }
            }
          }
        ]
      }
    },
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "blockUSButNotOROrWA"
    }
}
```

Como otro ejemplo, puede combinar la coincidencia geográfica con reglas basadas en tasas para priorizar los recursos para los usuarios de un país o región en particular. Puede crear una instrucción

basada en tasas diferente para cada instrucción de coincidencia geográfica o de etiquetas que utilice para diferenciar a sus usuarios. Establezca un límite de frecuencia mayor para los usuarios del país o región preferido y un límite de frecuencia menor para otros usuarios.

La siguiente lista de JSON muestra una regla de coincidencia geográfica seguida de reglas basadas en tasas que limitan la tasa de tráfico procedente de los Estados Unidos. Las normas permiten que el tráfico procedente de Oregón entre a una tasa mayor que el tráfico procedente de cualquier otro lugar del país.

```
{
  "Name": "geoMatchForLabels",
  "Priority": 190,
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ]
    }
  },
  "Action": {
    "Count": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "geoMatchForLabels"
  }
},
{
  "Name": "rateLimitOregon",
  "Priority": 195,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 3000,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "awswaf:clientip:geo:region:US-OR"
        }
      }
    }
  },
```

```
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rateLimitOregon"
  }
},
{
  "Name": "rateLimitUSNotOR",
  "Priority": 200,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "AndStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:clientip:geo:country:US"
              }
            },
            {
              "NotStatement": {
                "Statement": {
                  "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "awswaf:clientip:geo:region:US-OR"
                  }
                }
              }
            }
          ]
        }
      }
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
```

```
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rateLimitUSNotOR"
  }
}
```

Instrucción de regla de coincidencia de conjuntos de IP

La instrucción de coincidencia de conjuntos de IP inspecciona la dirección IP del origen de una solicitud web con un conjunto de direcciones IP y rangos de direcciones. Utilice esta opción para permitir o bloquear solicitudes web en función de las direcciones IP donde se originan las solicitudes. De forma predeterminada, AWS WAF usa la dirección IP del origen de la solicitud web, pero puede configurar la regla para que use un encabezado HTTP como `X-Forwarded-For` en su lugar.

AWS WAF admite todos los rangos CIDR de IPv4 e IPv6 excepto. `/0` Para obtener más información acerca de la notación CIDR, consulte la entrada de la Wikipedia Classless Inter-Domain Routing. Un conjunto de IP puede contener hasta 10 000 direcciones IP o rangos de direcciones IP para comprobarlos.

> **Note**
>
> Cada regla de coincidencia de conjuntos de IP hace referencia a un conjunto de IP, que se crea y mantiene independientemente de las reglas. Puede utilizar un único conjunto de direcciones IP en varias reglas y, al actualizar el conjunto al que se hace referencia, se AWS WAF actualizan automáticamente todas las reglas que hacen referencia a él.
> Para obtener información acerca de cómo se crea y se administra un conjunto de IP, consulte Crear y administrar un conjunto de IP.

Cuando añada o actualice las reglas en su grupo de reglas o ACL web, elija la opción IP set (Conjunto de IP) y seleccione el nombre del conjunto de IP que desea utilizar.

Se puede anidar: puede anidar este tipo de instrucción.

WCU: 1 WCU para la mayoría. Si configura la instrucción para usar direcciones IP reenviadas y especifica una posición de ANY, aumente el uso de las WCU en 4.

Esta instrucción utiliza la siguiente configuración:

- Especificación de conjunto de IP: elija el conjunto de IP que desea utilizar de la lista o cree uno nuevo.
- (Opcional) Configuración de IP reenviada: un nombre de encabezado de IP reenviado alternativo para usar en lugar del origen de la solicitud. Debe indicar si debe coincidir con la primera, la última o con cualquier otra dirección del encabezado. También puede especificar un comportamiento alternativo para aplicar a una solicitud web con una dirección IP malformada en la cabecera especificada. El comportamiento alternativo establece que el resultado de la solicitud coincide o no coincide. Para obtener más información, consulte Dirección IP reenviada.

Dónde encontrar esta instrucción de regla

- Generador de reglas en la consola: En Opción de la solicitud, elija Se origina desde una dirección IP de.
- Página Añadir mis propias reglas y grupos de reglas de la consola: elija la opción Conjunto de IP.
- API: IP SetReferenceStatement

Instrucción de regla de coincidencia de etiquetas

La instrucción de coincidencia de etiquetas inspecciona las etiquetas que se encuentran en la solicitud web comparándolas con una especificación de cadena. Las etiquetas que una regla puede inspeccionar son las que ya se han agregado a la solicitud web mediante otras reglas en la misma evaluación de la ACL web.

Las etiquetas no persisten fuera de la evaluación de la ACL web, pero puede acceder a las métricas de las etiquetas CloudWatch y ver los resúmenes de la información de las etiquetas de cualquier ACL web en la AWS WAF consola. Para más información, consulte Etiquetar métricas y dimensiones y Monitorización y ajuste. También se pueden ver etiquetas en los registros. Para obtener más información, consulte Campos de registro.

> **Note**
>
> Una instrucción de coincidencia de etiquetas Solamente puede ver las etiquetas de las reglas que se hayan evaluado anteriormente en la ACL web. Para obtener información sobre cómo AWS WAF se evalúan las reglas y los grupos de reglas en una ACL web, consulte. Procesamiento del orden de las reglas y los grupos de reglas en una ACL web

Para obtener más información sobre cómo agregar etiquetas y hacer que coincidan, consulte AWS WAF etiquetas en las solicitudes web.

Se puede anidar: puede anidar este tipo de instrucción.

WCU: 1 WCU

Esta instrucción utiliza la siguiente configuración:

- Alcance de coincidencia: configúrelo en Etiqueta para que coincida con el nombre de la etiqueta y, si lo desea, con los espacios de nombres y el prefijo anteriores. Configúrelo en Espacio de nombres para que coincida con algunas o todas las especificaciones del espacio de nombres y, opcionalmente, con el prefijo anterior.
- Clave: la cadena con la que desea hacer coincidir. Si especifica un alcance de coincidencia de espacio de nombres, solo debe especificar los espacios de nombres y, opcionalmente, el prefijo, con dos puntos al final. Si especifica un alcance de coincidencia de etiquetas, este debe incluir el nombre de la etiqueta y, de forma opcional, puede incluir los espacios de nombres y el prefijo anteriores.

Para obtener más información sobre estas opciones, consulte AWS WAF reglas que coinciden con las etiquetas y AWS WAF ejemplos de concordancia de etiquetas.

Dónde encontrar esta instrucción de regla

- Generador de reglas en la consola: En Opción de la solicitud, elija Tiene etiqueta.
- API: LabelMatchStatement

Instrucción de regla de coincidencia de expresiones regulares

Una sentencia de coincidencia de expresiones regulares indica que se debe AWS WAF hacer coincidir un componente de solicitud con una sola expresión regular (regex). Una solicitud web coincide con la instrucción si el componente de la solicitud coincide con la regex que especificó.

Este tipo de instrucción es una buena alternativa Instrucción de regla de coincidencia de conjuntos de patrones de regex para las situaciones en las que desee combinar los criterios de coincidencia mediante la lógica matemática. Por ejemplo, si desea que un componente de la solicitud coincida con algunos patrones de regex y no con otros, puede combinar las instrucciones de coincidencia de regex utilizando Instrucción de reglas de AND y Instrucción de reglas de NOT.

AWS WAF admite la sintaxis de patrones utilizada por la biblioteca PCRE con algunas excepciones. `libpcre` La biblioteca está documentada en PCRE, expresiones regulares compatibles con Perl. Para obtener información sobre el AWS WAF soporte, consulteCoincidencia de patrones de expresiones regulares en AWS WAF.

Se puede anidar: puede anidar este tipo de instrucción.

WCU: 3 WCU, como coste base. Si utiliza el componente de solicitud Todos los parámetros de consulta, añada 10 WCU. Si utiliza el Cuerpo JSON del componente de la solicitud, duplique el coste base de las WCU. Para cada Transformación de texto que aplique, añada 10 WCU.

Este tipo de instrucción funciona en un componente de solicitud web y requiere la siguiente configuración del componente de la solicitud:

- Componente de solicitud: la parte de la solicitud web que se va a inspeccionar, por ejemplo, una cadena de consulta o el cuerpo.

  > **Warning**
  >
  > Si inspeccionas el cuerpo, el cuerpo de JSON, los encabezados o las cookies de los componentes de la solicitud, consulta las limitaciones en cuanto a la cantidad de contenido que AWS WAF se puede inspeccionar. Manejo de componentes de solicitudes sobredimensionadas en AWS WAF

  Para obtener información sobre los componentes de la solicitud web, consulte Especificación y manejo de componentes de solicitudes web.
- Transformaciones de texto opcionales: transformaciones que desea AWS WAF realizar en el componente de la solicitud antes de inspeccionarlo. Por ejemplo, puede convertir a minúsculas o normalizar el espacio en blanco. Si especifica más de una transformación, las AWS WAF procesa en el orden indicado. Para obtener más información, consulte Opciones de transformación de texto.

Dónde encontrar esta instrucción de regla

- Generador de reglas en la consola: en Tipo de coincidencia, seleccione Coincide con expresión regular.
- API: RegexMatchStatement

Instrucción de regla de coincidencia de conjuntos de patrones de regex

La comparación del conjunto de patrones de expresiones regulares inspecciona la parte de la solicitud web que especifica para los patrones de expresiones regulares que ha especificado en un conjunto de patrones de expresiones regulares.

AWS WAF admite la sintaxis de patrones utilizada por la biblioteca PCRE `libpcre` con algunas excepciones. La biblioteca está documentada en PCRE, expresiones regulares compatibles con Perl. Para obtener información sobre el AWS WAF soporte, consulteCoincidencia de patrones de expresiones regulares en AWS WAF.

> **Note**
>
> Cada regla de coincidencia de conjuntos de patrones de regex hace referencia a un conjunto de patrones de regex, que se crea y mantiene independientemente de las reglas. Puede utilizar un único conjunto de patrones de expresiones regulares en varias reglas y, al actualizar el conjunto al que se hace referencia, se AWS WAF actualizan automáticamente todas las reglas que hacen referencia a él.
> Para obtener más información acerca de cómo se crea y administra un conjunto de patrones regex, consulte Crear y administrar un conjunto de patrones de expresiones regex.

Una sentencia de coincidencia de conjuntos de patrones de expresiones regulares indica AWS WAF que hay que buscar cualquiera de los patrones del conjunto dentro del componente de solicitud que elija. Una solicitud web coincidirá con la instrucción de la regla del conjunto de patrones si el componente de la solicitud coincide con cualquiera de los patrones del conjunto.

Si desea combinar sus coincidencias de patrones de regex utilizando la lógica, por ejemplo, para que coincidan con algunas expresiones regulares y no con otras, considere la posibilidad de utilizar Instrucción de regla de coincidencia de expresiones regulares.

Se puede anidar: puede anidar este tipo de instrucción.

WCU: 25 WCU, como coste base. Si utiliza el componente de solicitud Todos los parámetros de consulta, añada 10 WCU. Si utiliza el Cuerpo JSON del componente de la solicitud, duplique el coste base de las WCU. Para cada Transformación de texto que aplique, añada 10 WCU.

Este tipo de instrucción funciona en un componente de solicitud web y requiere la siguiente configuración del componente de la solicitud:

- Componente de solicitud: la parte de la solicitud web que se va a inspeccionar, por ejemplo, una cadena de consulta o el cuerpo.

  > **Warning**
  >
  > Si inspeccionas el cuerpo, el cuerpo de JSON, los encabezados o las cookies de los componentes de la solicitud, consulta las limitaciones en cuanto a la cantidad de contenido AWS WAF que se puede inspeccionar. Manejo de componentes de solicitudes sobredimensionadas en AWS WAF

  Para obtener información sobre los componentes de la solicitud web, consulte Especificación y manejo de componentes de solicitudes web.

- Transformaciones de texto opcionales: transformaciones que desea AWS WAF realizar en el componente de la solicitud antes de inspeccionarlo. Por ejemplo, puede convertir a minúsculas o normalizar el espacio en blanco. Si especifica más de una transformación, las AWS WAF procesa en el orden indicado. Para obtener más información, consulte Opciones de transformación de texto.

Esta instrucción requiere la siguiente configuración:

- Especificación de conjunto de patrones de regex: Elija el conjunto de patrones de regex que desea utilizar de la lista o cree uno nuevo.

Dónde encontrar esta instrucción de regla

- Generador de reglas en la consola: En Tipo de coincidencia, elija Condición de coincidencia de cadena > Coincide con el patrón del conjunto de expresiones regulares.
- API: RegexPatternSetReferenceStatement

Instrucción de regla de restricción de tamaño

Una instrucción de restricción de tamaño compara el número de bytes de un componente de solicitud web con el número que proporcione y coincide según sus criterios de comparación. El criterio de comparación es un operador como mayor que (>) o menor que (<). Por ejemplo, puede hacer coincidir las solicitudes que tienen una cadena de consulta con un tamaño superior a 100 bytes.

> **Note**
>
> Esta instrucción solo inspecciona el tamaño del componente de la solicitud web. No inspecciona el contenido del componente.

Si inspecciona la ruta de URI, cualquier `/` en la ruta cuenta como un carácter. Por ejemplo, el `/logo.jpg` de la ruta del URI tiene nueve caracteres.

Se puede anidar: puede anidar este tipo de instrucción.

WCU: 1 WCU, como coste base. Si utiliza el componente de solicitud Todos los parámetros de consulta, añada 10 WCU. Si utiliza el Cuerpo JSON del componente de la solicitud, duplique el coste base de las WCU. Para cada Transformación de texto que aplique, añada 10 WCU.

Este tipo de instrucción funciona en un componente de solicitud web y requiere la siguiente configuración del componente de la solicitud:

- Componente de solicitud: la parte de la solicitud web que se va a inspeccionar, por ejemplo, una cadena de consulta o el cuerpo. Para obtener información sobre los componentes de la solicitud web, consulte Especificación y manejo de componentes de solicitudes web.

  Una instrucción de restricción de tamaño inspecciona solo el tamaño del componente después de aplicar cualquier transformación. No inspecciona el contenido del componente.
- Transformaciones de texto opcionales: transformaciones que desea AWS WAF realizar en el componente de la solicitud antes de inspeccionar su tamaño. Por ejemplo, puede comprimir espacios en blanco o decodificar entidades HTML. Si especifica más de una transformación, las AWS WAF procesa en el orden indicado. Para obtener más información, consulte Opciones de transformación de texto.

Además, esta instrucción requiere la siguiente configuración:

- Condición de coincidencia de tamaño: indica el operador de comparación numérica que se utilizará para comparar el tamaño que proporciona con el componente de solicitud que ha elegido. Elija el operador de la lista.
- Tamaño: el ajuste de tamaño, en bytes que se usará en la comparación.

Dónde encontrar esta instrucción de regla

- Generador de reglas en la consola: En Tipo de coincidencia, en Condición de coincidencia de tamaño, elija la condición que quiere usar.
- API: SizeConstraintStatement

Instrucción de regla de ataques de inyecciones SQL

Una instrucción de regla de inyección de código SQL inspecciona en busca de código SQL malicioso. Los atacantes insertan código SQL malicioso en solicitudes web con el objetivo de modificar su base de datos o extraer datos de ella.

Se puede anidar: puede anidar este tipo de instrucción.

WCU: el coste base depende del nivel de sensibilidad establecido para la instrucción de regla: Low cuesta 20 y High cuesta 30.

Si utiliza el componente de solicitud Todos los parámetros de consulta, añada 10 WCU. Si utiliza el Cuerpo JSON del componente de la solicitud, duplique el coste base de las WCU. Para cada Transformación de texto que aplique, añada 10 WCU.

Este tipo de instrucción funciona en un componente de solicitud web y requiere la siguiente configuración del componente de la solicitud:

- Componente de solicitud: la parte de la solicitud web que se va a inspeccionar, por ejemplo, una cadena de consulta o el cuerpo.

  > **Warning**
  >
  > Si inspeccionas el cuerpo, el cuerpo de JSON, los encabezados o las cookies de los componentes de la solicitud, consulta las limitaciones en cuanto a la cantidad de contenido que AWS WAF se puede inspeccionar. Manejo de componentes de solicitudes sobredimensionadas en AWS WAF

  Para obtener información sobre los componentes de la solicitud web, consulte Especificación y manejo de componentes de solicitudes web.
- Transformaciones de texto opcionales: transformaciones que desea AWS WAF realizar en el componente de la solicitud antes de inspeccionarlo. Por ejemplo, puede convertir a minúsculas o

normalizar el espacio en blanco. Si especifica más de una transformación, las AWS WAF procesa en el orden indicado. Para obtener más información, consulte Opciones de transformación de texto.

Además, esta instrucción requiere la siguiente configuración:

- Nivel de sensibilidad: esta configuración ajusta la sensibilidad de los criterios de coincidencia de las inyecciones de código SQL. Las opciones son LOW y HIGH. El ajuste predeterminado es LOW.

  La configuración HIGH detecta más ataques de inyección de código SQL y es la configuración recomendada. Debido a la mayor sensibilidad, esta configuración genera más falsos positivos, especialmente si las solicitudes web suelen contener cadenas inusuales. Durante las pruebas y ajustes de la ACL web, es posible que tenga que esforzarse más para mitigar los falsos positivos. Para obtener más información, consulte Probando y ajustando sus AWS WAF protecciones.

  La configuración más baja proporciona una detección de inyecciones de código SQL menos rigurosa, lo que también se traduce en menos falsos positivos. LOW puede ser una mejor opción para los recursos que tienen otras protecciones contra los ataques de inyección de código SQL o que tienen una baja tolerancia a los falsos positivos.

Dónde encontrar esta instrucción de regla

- Generador de reglas en la consola: Tipo de coincidencia, elija Condiciones de coincidencia de ataques > Contiene ataques de inyección de código SQL).
- API: SqliMatchStatement

Instrucción de regla de coincidencia de cadenas

Una sentencia de coincidencia de cadenas indica la cadena que AWS WAF desea buscar en una solicitud, en qué parte de la solicitud se va a buscar y cómo. Por ejemplo, puede buscar una cadena específica al inicio de cualquier cadena de consulta de la solicitud o como una coincidencia exacta para el encabezado `User-agent` de la solicitud. Normalmente, la cadena se compone de caracteres ASCII imprimibles, pero puede usar cualquier carácter comprendido entre los valores hexadecimales 0x00 y 0xFF (valores decimales 0 a 255).

Se puede anidar: puede anidar este tipo de instrucción.

WCU: el coste base depende del tipo de coincidencia que utilice.

- Coincide exactamente con la cadena: 2
- Comienza con la cadena: 2
- Acaba con la cadena: 2
- Contiene la cadena: 10
- Contiene la palabra: 10

Si utiliza el componente de solicitud Todos los parámetros de consulta, añada 10 WCU. Si utiliza el Cuerpo JSON del componente de la solicitud, duplique el coste base de las WCU. Para cada Transformación de texto que aplique, añada 10 WCU.

Este tipo de instrucción funciona en un componente de solicitud web y requiere la siguiente configuración del componente de la solicitud:

- Componente de solicitud: la parte de la solicitud web que se va a inspeccionar, por ejemplo, una cadena de consulta o el cuerpo.

  > **Warning**
  >
  > Si inspeccionas el cuerpo, el cuerpo de JSON, los encabezados o las cookies de los componentes de la solicitud, consulta las limitaciones en cuanto a la cantidad de contenido que AWS WAF se puede inspeccionar. Manejo de componentes de solicitudes sobredimensionadas en AWS WAF

  Para obtener información sobre los componentes de la solicitud web, consulte Especificación y manejo de componentes de solicitudes web.
- Transformaciones de texto opcionales: transformaciones que desea AWS WAF realizar en el componente de la solicitud antes de inspeccionarlo. Por ejemplo, puede convertir a minúsculas o normalizar el espacio en blanco. Si especifica más de una transformación, las AWS WAF procesa en el orden indicado. Para obtener más información, consulte Opciones de transformación de texto.

Además, esta instrucción requiere la siguiente configuración:

- Cadena que debe coincidir: es la cadena que desea AWS WAF comparar con el componente de solicitud especificado. Normalmente, la cadena se compone de caracteres ASCII imprimibles, pero

puede usar cualquier carácter comprendido entre los valores hexadecimales 0x00 y 0xFF (valores decimales 0 a 255).

- Condición de coincidencia de cadenas: indica el tipo de búsqueda que AWS WAF desea realizar.
  - Coincide exactamente con la cadena: la cadena y el valor del componente de la solicitud son idénticas.
  - Empieza con la cadena: la cadena aparece al principio del componente de solicitud.
  - Acaba con la cadena: la cadena aparece al final del componente de solicitud.
  - Contiene la cadena: la cadena aparece en cualquier parte del componente de la solicitud.
  - Contiene palabras: la cadena que especifique debe aparecer en el componente de la solicitud.

    Para esta opción, la cadena que especifique Solamente puede contener caracteres alfanuméricos o guion bajo (A-Z, a-z, 0-9 o _).

    Debe cumplirse una de las siguientes condiciones para que la solicitud coincida:
    - La cadena coincide exactamente con el valor del componente de solicitud, como el valor de un encabezado.
    - La cadena está al principio del componente de solicitud y le sigue un carácter que no es alfanumérico ni guion bajo (_), por ejemplo, `BadBot;`.
    - La cadena está al final del componente de solicitud y le precede un carácter que no es alfanumérico ni guion bajo (_), por ejemplo, `;BadBot`.
    - La cadena está en la mitad del componente de solicitud y va precedida y seguida de caracteres que no son alfanuméricos ni guion bajo (_), por ejemplo, `-BadBot;`.

Dónde encontrar esta instrucción de regla

- Generador de reglas en la consola: en Tipo de coincidencia, elija Condición de coincidencia de cadena y, a continuación, rellene las cadenas con las que quiere que coincida.
- API: ByteMatchStatement

Instrucción de regla de ataques de scripting entre sitios

Una instrucción de ataque XSS (scripting entre sitios) busca scripts maliciosos en un componente de solicitud web. En un ataque de XSS, el atacante utiliza vulnerabilidades en un sitio web benigno como vehículo para inyectar scripts maliciosos del sitio de cliente en otros navegadores web legítimos.

Se puede anidar: puede anidar este tipo de instrucción.

WCU: 40 WCU, como coste base. Si utiliza el componente de solicitud Todos los parámetros de consulta, añada 10 WCU. Si utiliza el Cuerpo JSON del componente de la solicitud, duplique el coste base de las WCU. Para cada Transformación de texto que aplique, añada 10 WCU.

Este tipo de instrucción funciona en un componente de solicitud web y requiere la siguiente configuración del componente de la solicitud:

- Componente de solicitud: la parte de la solicitud web que se va a inspeccionar, por ejemplo, una cadena de consulta o el cuerpo.

  > **Warning**
  >
  > Si inspeccionas el cuerpo, el cuerpo de JSON, los encabezados o las cookies de los componentes de la solicitud, consulta las limitaciones en cuanto a la cantidad de contenido que AWS WAF se puede inspeccionar. Manejo de componentes de solicitudes sobredimensionadas en AWS WAF

  Para obtener información sobre los componentes de la solicitud web, consulte Especificación y manejo de componentes de solicitudes web.
- Transformaciones de texto opcionales: transformaciones que desea AWS WAF realizar en el componente de la solicitud antes de inspeccionarlo. Por ejemplo, puede convertir a minúsculas o normalizar el espacio en blanco. Si especifica más de una transformación, las AWS WAF procesa en el orden indicado. Para obtener más información, consulte Opciones de transformación de texto.

Dónde encontrar esta instrucción de regla

- Generador de reglas en la consola: En Tipo de coincidencia, elija Condiciones de coincidencia de ataques > Contiene ataques de inyección de código XSS).
- API: XssMatchStatement

instrucciones de reglas lógicas

Las instrucciones de reglas lógicas le permiten combinar otras instrucciones o negar sus resultados. Cada instrucción de regla lógica necesita al menos una instrucción anidada.

Para combinar los resultados de las instrucciones de reglas, anide las instrucciones en instrucciones de reglas lógicas.

Las instrucciones de reglas lógicas se pueden anidar. Puede anidarlas dentro de otras sentencias de reglas lógicas y utilizarlas en sentencias de ámbito reducido. Para obtener información sobre las instrucciones de restricción de acceso, consulte Instrucciones de restricción de acceso.

> **Note**
>
> El editor visual de la consola admite un nivel de anidamiento de instrucciones de reglas, que funciona para muchas necesidades. Para anidar más niveles, edite la representación JSON de la regla en la consola o use las API.

Esta tabla describe las instrucciones de regla lógica y proporciona pautas para calcular el uso de unidades de capacidad de ACL web (WCU) para cada una. Para obtener información acerca de las WCU, consulte AWS WAF unidades de capacidad ACL web (WCU).

Instrucción lógica	Descripción	WCU
Lógica de AND	Combina instrucciones anidadas con lógica AND.	Se basa en instrucciones anidadas
Lógica de NOT	Niega los resultados de una instrucción anidada.	Se basa en una instrucción anidada
Lógica de OR	Combina instrucciones anidadas con lógica OR.	Se basa en instrucciones anidadas

Instrucción de reglas de AND

La instrucción de regla AND combina instrucciones anidadas con una operación AND lógica, por lo que todas las instrucciones anidadas deben coincidir para que la instrucción AND coincida. Esto requiere al menos dos declaraciones anidadas.

Se puede anidar: puede anidar este tipo de instrucción.

WCU: depende de las instrucciones anidadas.

Dónde encontrar esta instrucción de regla

- Generador de reglas en la consola: en Si una solicitud, elija coincide con todas las instrucciones (AND) y, a continuación, rellene las instrucciones anidadas.
- API — AndStatement

Ejemplos

La siguiente lista muestra el uso de AND y las instrucciones de regla lógica NOT para eliminar los falsos positivos de las coincidencias de una instrucción de ataque de inyección de código SQL. En este ejemplo, supongamos que podemos escribir una instrucción de coincidencia de un solo byte para que coincida con las solicitudes que generan falsos positivos.

La instrucción AND coincide con las solicitudes que no coinciden con la instrucción de coincidencia de bytes y que sí coinciden con la instrucción de ataque de inyección de código SQL.

```
{
      "Name": "SQLiExcludeFalsePositives",
      "Priority": 0,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "NotStatement": {
                "Statement": {
                  "ByteMatchStatement": {
                    "SearchString": "string identifying a false positive",
                    "FieldToMatch": {
                      "Body": {
                        "OversizeHandling": "MATCH"
                      }
```

```
                    },
                    "TextTransformations": [
                      {
                        "Priority": 0,
                        "Type": "NONE"
                      }
                    ],
                    "PositionalConstraint": "CONTAINS"
                  }
                }
              }
            },
            {
              "SqliMatchStatement": {
                "FieldToMatch": {
                  "Body": {
                    "OversizeHandling": "MATCH"
                  }
                },
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "SQLiExcludeFalsePositives"
      }
    }
```

Con el editor visual de reglas de la consola, puede anidar una instrucción no lógica o una instrucción NOT en una instrucción OR o AND. La anidación de la instrucción NOT se muestra en el ejemplo anterior.

Con el editor visual de reglas de la consola, puede anidar la mayoría de las instrucciones anidables en una instrucción de regla lógica, como la que se muestra en el ejemplo anterior. No puede usar el editor visual para anidar instrucciones OR o AND. Para configurar este tipo de anidación, debe proporcionar la instrucción de la regla en JSON. Por ejemplo, la siguiente lista de reglas JSON incluye una instrucción OR anidada dentro de una instrucción AND.

```
{
  "Name": "match_rule",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        },
        {
          "OrStatement": {
            "Statements": [
              {
                "GeoMatchStatement": {
                  "CountryCodes": [
                    "JM",
                    "JP"
                  ]
                }
              },
              {
                "ByteMatchStatement": {
                  "SearchString": "JCountryString",
                  "FieldToMatch": {
```

```
                    "Body": {}
                  },
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
                  ],
                  "PositionalConstraint": "CONTAINS"
                }
              }
            ]
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

Instrucción de reglas de NOT

La instrucción de regla NOT niega lógicamente los resultados de una sola instrucción anidada, por lo que las instrucciones anidadas no deben coincidir para que la instrucción NOT coincida y viceversa. Requiere una instrucción anidada.

Por ejemplo, si desea bloquear las solicitudes que no provienen de un país específico, cree una instrucción NOT con la acción establecida en bloquear y anide una instrucción de coincidencia geográfica que especifique el país.

Se puede anidar: puede anidar este tipo de instrucción.

WCU: depende de las instrucción anidada.

Dónde encontrar esta instrucción de regla

- Generador de reglas en la consola: en Si una solicitud, elija no coincide con la instrucción (NOT) y, a continuación, rellene las instrucciones anidadas.
- API — NotStatement

Instrucción de reglas de OR

La instrucción de regla OR combina instrucciones anidadas con lógica OR, por lo que una de las instrucciones anidadas debe coincidir para que la instrucción OR coincida. Esto requiere al menos dos declaraciones anidadas.

Por ejemplo, si desea bloquear las solicitudes procedentes de un país específico o que contengan una cadena de consulta específica, puede crear una instrucción OR y anidar en ella una instrucción de coincidencia geográfica para el país y una instrucción de coincidencia de cadena para la cadena de consulta.

Si, como alternativa, desea bloquear las solicitudes que no provienen de un país específico o que contengan una cadena de consulta específica, modifique la instrucción OR anterior para anidar la instrucción de coincidencia geográfica en un nivel inferior, dentro de una instrucción NOT. Este nivel de anidamiento requiere que utilice el formato JSON, ya que la consola solo admite un nivel de anidamiento.

Se puede anidar: puede anidar este tipo de instrucción.

WCU: depende de las instrucciones anidadas.

Dónde encontrar esta instrucción de regla

- Generador de reglas en la consola: en Si una solicitud, elija coincide con al menos una de las instrucciones (OR) y, a continuación, rellene las instrucciones anidadas.
- API — OrStatement

Ejemplos

La siguiente lista muestra el uso de OR para combinar otras dos instrucciones. La instrucción OR coincide si alguna de las instrucciones anidadas coincide.

```
{
  "Name": "neitherOfTwo",
```

```
  "Priority": 1,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "neitherOfTwo"
  },
  "Statement": {
    "OrStatement": {
      "Statements": [
        {
          "GeoMatchStatement": {
            "CountryCodes": [
              "CA"
            ]
          }
        },
        {
          "IPSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/ipset/test-ip-
set-22222222/33333333-4444-5555-6666-777777777777"
          }
        }
      ]
    }
  }
}
```

Con el editor visual de reglas de la consola, puede anidar la mayoría de las instrucciones anidables en una instrucción de regla lógica, pero no puede utilizar el editor visual para anidar instrucciones OR o AND. Para configurar este tipo de anidación, debe proporcionar la instrucción de la regla en JSON. Por ejemplo, la siguiente lista de reglas JSON incluye una instrucción OR anidada dentro de una instrucción AND.

```
{
  "Name": "match_rule",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
```

```
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        },
        {
          "OrStatement": {
            "Statements": [
              {
                "GeoMatchStatement": {
                  "CountryCodes": [
                    "JM",
                    "JP"
                  ]
                }
              },
              {
                "ByteMatchStatement": {
                  "SearchString": "JCountryString",
                  "FieldToMatch": {
                    "Body": {}
                  },
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
                  ],
                  "PositionalConstraint": "CONTAINS"
                }
              }
            ]
          }
        }
```

```
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

Instrucción de regla basada en frecuencia

Una regla basada en tasas cuenta las solicitudes entrantes y las solicitudes de límites de tasa cuando llegan a una tasa demasiado rápida. La regla agrega las solicitudes según sus criterios y cuenta y limita las agrupaciones agregadas en función del período de evaluación de la regla, el límite de solicitudes y la configuración de las acciones.

> **Note**
>
> También puedes limitar la frecuencia de las solicitudes web utilizando el nivel de protección específico del grupo de reglas AWS gestionadas por el control de bots. El uso de este grupo de reglas gestionado conlleva cargos adicionales. Para obtener más información, consulte Opciones para limitar las tasas en las reglas basadas en tasas y en las reglas específicas de control de bots.

AWS WAF rastrea y administra las solicitudes web por separado para cada instancia de una regla basada en tarifas que utilices. Por ejemplo, si proporciona la misma configuración de reglas basadas en tasas en dos ACL web, cada una de las dos sentencias de regla representa una instancia independiente de la regla basada en tasas y cada una recibe su propio seguimiento y administración. AWS WAF Si define una regla basada en tasas dentro de un grupo de reglas y, a continuación, usa ese grupo de reglas en varios lugares, cada uso crea una instancia independiente de la regla basada en tasas que se encarga de su propio seguimiento y administración. AWS WAF

No se puede anidar: no se puede anidar este tipo de instrucción en otras instrucciones. Puede incluirlo directamente en una ACL web o en un grupo de reglas.

Declaración de alcance reducido: este tipo de regla puede adoptar una declaración de alcance reducido para reducir el alcance de las solicitudes que la regla rastrea y los límites de frecuencia. La declaración de reducción del alcance puede ser opcional u obligatoria, en función de las demás opciones de configuración de la regla. Los detalles se describen en esta sección. Para obtener información general sobre las declaraciones de alcance reducido, consulte. Instrucciones de restricción de acceso

WCU: 2 WCU, como coste base. Para cada clave de agregación personalizada que especifique, añada 30 WCU. Si utiliza una instrucción de restricción de acceso en la regla, calcule y agregue las WCU correspondientes.

Dónde encontrar esta instrucción de regla

- Generador de reglas en la web de ACL: En Regla, en Tipo, elija Regla basada en tasas.
- API — RateBasedStatement

Temas

- Configuración de alto nivel de la regla basada en tasas
- Advertencias sobre las reglas basadas en tarifas
- Opciones y claves de agregación de reglas basadas en tasas
- Instancias y recuentos de agregación de reglas basados en tasas
- Comportamiento de limitación de velocidad de solicitud de reglas basadas en la tasa
- Ejemplos de reglas basadas en tasas
- Lista de direcciones IP cuyas tasas están limitada por reglas basadas en tasas

Configuración de alto nivel de la regla basada en tasas

Una declaración de regla basada en tasas utiliza la siguiente configuración de alto nivel:

- Ventana de evaluación: la cantidad de tiempo, en segundos, que AWS WAF debe incluirse en sus recuentos de solicitudes, si se compara con la hora actual. Por ejemplo, si el valor es 120, al AWS WAF comprobar la tasa, se cuentan las solicitudes de los 2 minutos inmediatamente anteriores a la hora actual. Los valores válidos son 60 (1 minuto), 120 (2 minutos), 300 (5 minutos) y 600 (10 minutos), y 300 (5 minutos) es el valor predeterminado.

Esta configuración no determina con qué frecuencia se AWS WAF comprueba la velocidad, sino qué tan atrás se mira cada vez que se comprueba. AWS WAF comprueba la tasa con frecuencia, con una temporización independiente de la configuración de la ventana de evaluación.

- Límite de frecuencia: el número máximo de solicitudes que coinciden con sus criterios y que solo se AWS WAF deben registrar durante el período de evaluación especificado. El límite mínimo permitido es 100. Cuando se supera este límite, se AWS WAF aplica la configuración de acción de la regla a las solicitudes adicionales que coincidan con tus criterios.

  AWS WAF aplica un límite de velocidad cercano al límite que hayas establecido, pero no garantiza una coincidencia exacta del límite. Para obtener más información, consulte Advertencias sobre las reglas basadas en tarifas.
- Agregación de solicitudes: los criterios de agregación que se utilizan en las solicitudes web exigen que la regla basada en tasas cuente y limite las tasas. El límite de velocidad que establezca se aplica a cada instancia de agregación. Para más detalles, consulte Claves y opciones de agregación y Recuentos e instancias de agregación.
- Acción: la acción que se debe realizar cuando se solicita que la regla limite las tasas. Puede utilizar cualquier acción de regla excepto Allow. Se establece a nivel de reglas, como de costumbre, pero tiene algunas restricciones y comportamientos que son específicos de las reglas basadas en tasas. Para obtener información general sobre las acciones de las reglas, consulte Acción de regla. Para obtener información específica sobre la limitación de velocidad, consulta Comportamiento de limitación de velocidad de solicitud de reglas basadas en la tasa esta sección.
- Alcance de la inspección y limitación de la tasa: puede reducir el alcance de las solicitudes que la instrucción basada en tasas rastrea y los límites de tasas añadiendo una instrucción de restricción de acceso. Si especifica una instrucción de restricción de acceso, la regla solo agrega, cuenta y limita las tasas de las solicitudes que coinciden con la instrucción de restricción de acceso. Si elige la opción de agregación de solicitudes Contar todas, se requiere la instrucción de restricción de acceso. Para obtener más información sobre las instrucciones de restricción de acceso, consulte Instrucciones de restricción de acceso.
- Configuración de IP reenviada (opcional): solo se usa si especifica la dirección IP en el encabezado de la agregación de solicitudes, ya sea por sí sola o como parte de la configuración de claves personalizadas. AWS WAF recupera la primera dirección IP del encabezado especificado y la utiliza como valor de agregación. Un encabezado común para este propósito es `X-Forwarded-For`, pero puede especificar cualquier encabezado. Para obtener más información, consulte Dirección IP reenviada.

Advertencias sobre las reglas basadas en tarifas

AWS WAF La limitación de velocidad está diseñada para controlar las altas tasas de solicitudes y proteger la disponibilidad de la aplicación de la manera más eficiente y eficaz posible. No está diseñada para limitar de forma precisa la tasa de solicitudes.

- AWS WAF estima la tasa de solicitudes actual mediante un algoritmo que da más importancia a las solicitudes más recientes. Por este motivo, AWS WAF aplicará un límite de velocidad cercano al límite que hayas establecido, pero no garantiza una coincidencia exacta del límite.
- Cada vez que AWS WAF calcule la tasa de solicitudes, AWS WAF analiza el número de solicitudes recibidas durante el período de evaluación configurado. Debido a este y a otros factores, como los retrasos en la propagación, es posible que las solicitudes lleguen a una velocidad demasiado alta durante varios minutos antes de que las AWS WAF detecte y limite la frecuencia. Del mismo modo, la tasa de solicitudes puede estar por debajo del límite durante un período de tiempo antes de que AWS WAF detecte la disminución e interrumpa la acción de limitación de la velocidad. Por lo general, este retraso es inferior a 30 segundos.
- Si cambias alguno de los ajustes del límite de velocidad de una regla que está en uso, el cambio restablece los recuentos de límites de velocidad de la regla. Esto puede detener las actividades de limitación de velocidad de la regla durante un máximo de un minuto. Los ajustes del límite de velocidad son la ventana de evaluación, el límite de velocidad, los ajustes de agregación de solicitudes, la configuración de la IP reenviada y el alcance de la inspección.

Opciones y claves de agregación de reglas basadas en tasas

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. Puede configurar la regla para que utilice otras claves de agregación y combinaciones de claves. Por ejemplo, puede agregar en función de una dirección IP reenviada, del método HTTP o de un argumento de consulta. También puede especificar combinaciones de claves de agregación, como la dirección IP y el método HTTP, o los valores de dos cookies diferentes.

> **Note**
>
> Todos los componentes de la solicitud que especifique en la clave de agregación deben estar presentes en una solicitud web para que la solicitud se evalúe o se limite su tasa según la regla.

Puede configurar la regla basada en tasas con las siguientes opciones de agregación.

- Dirección IP de origen: agregue usando solo la dirección IP del origen de la solicitud web.

  Es posible que la dirección IP de origen no contenga la dirección del cliente de origen. Si una solicitud web pasa por uno o más proxies o equilibradores de carga, contendrá la dirección del último proxy.
- Dirección IP en encabezado: agregue solo una dirección de cliente en un encabezado HTTP. También se denomina dirección IP reenviada.

  Con esta configuración, también se especifica un comportamiento alternativo para aplicarlo a una solicitud web con una dirección IP con un formato incorrecto en el encabezado. El comportamiento alternativo establece que el resultado de la solicitud coincide o no coincide. Si no hay coincidencia, la regla basada en tasas no cuenta ni limita la tasa de la solicitud. En caso de coincidencia, la regla basada en tasas agrupa la solicitud junto con otras solicitudes que tienen una dirección IP con formato incorrecto en el encabezado especificado.

  Tenga cuidado con esta opción, ya que los proxies pueden gestionar los encabezados de forma incoherente y también pueden modificarse para evitar la inspección. Consulte Dirección IP reenviada para obtener más información y las prácticas recomendadas.
- Contar todas: cuente y limite las tasas de todas las solicitudes que coincidan con la instrucción de restricción de acceso de la regla. Esta opción requiere una instrucción de restricción de acceso. Por lo general, se usa para limitar las tasas de un conjunto específico de solicitudes, como todas las solicitudes con una etiqueta específica o todas las solicitudes de un área geográfica específica.
- Claves personalizadas: agréguelas mediante una o más claves de agregación personalizadas. Para combinar cualquiera de las opciones de direcciones IP con otras claves de agregación, defínalas aquí en las claves personalizadas.

  Las claves de agregación personalizadas son un subconjunto de las opciones de los componentes de solicitudes web que se describen en Opciones de componentes de solicitudes.

  Las opciones principales son las siguientes. Excepto donde se indique lo contrario, puede usar una opción varias veces, por ejemplo, dos encabezados o tres espacios de nombres de etiquetas.
  - Espacio de nombres de etiquetas: utilice un espacio de nombres de etiquetas como una clave de agregación. Cada nombre de etiqueta totalmente cualificado que tenga el espacio de nombres de etiqueta especificado contribuye a la instancia de agregación. Si usa solo un espacio de nombres de etiquetas como clave personalizada, cada nombre de etiqueta define completamente una instancia de agregación.

La regla basada en tasas usa solo las etiquetas que se han agregado a la solicitud mediante reglas que se han evaluado de antemano en la ACL web.

Para obtener información acerca de los espacios de nombres y los nombres de las etiquetas, consulte AWS WAF requisitos de nomenclatura y sintaxis de etiquetas.

- Encabezado: utilice un encabezado con nombre como clave de agregación. Cada valor distinto del encabezado contribuye a la instancia de agregación.

  El encabezado realiza una transformación de texto opcional. Consulte Opciones de transformación de texto.

- Cookie: utilice una cookie con nombre como clave de agregación. Cada valor distinto de la cookie contribuye a la instancia de agregación.

  La cookie realiza una transformación de texto opcional. Consulte Opciones de transformación de texto.

- Argumento de consulta: utilice un único argumento de consulta en la solicitud como clave de agregación. Cada valor distinto del argumento de consulta mencionado contribuye a la instancia de agregación.

  El argumento de consulta realiza una transformación de texto opcional. Consulte Opciones de transformación de texto.

- Cadena de consulta: utilice toda la cadena de consulta de la solicitud como clave de agregación. Cada cadena de consulta distinta contribuye a la instancia de agregación. Puede usar este tipo de clave una vez.

  La cadena de consulta realiza una transformación de texto opcional. Consulte Opciones de transformación de texto.

- Ruta de URI: use la ruta de URI de la solicitud como clave agregada. Cada ruta del URI diferente contribuye a la instancia de agregación. Puede usar este tipo de clave una vez.

  La ruta del URI realiza una transformación de texto opcional. Consulte Opciones de transformación de texto.

- Método HTTP: use el método HTTP de la solicitud como clave de agregación. Cada método de HTTP diferenciado contribuye a la instancia de agregación. Puede usar este tipo de clave una vez.

- Dirección IP: agregue usando la dirección IP del origen de la solicitud web en combinación con otras claves.

  Es posible que no contenga la dirección del cliente de origen. Si una solicitud web pasa por uno o más proxies o equilibradores de carga, contendrá la dirección del último proxy.
- Dirección IP en el encabezado: agregue la dirección del cliente en un encabezado HTTP en combinación con otras claves. También se denomina dirección IP reenviada.

  Tenga cuidado con esta opción, ya que los proxies pueden gestionar los encabezados de forma incoherente y pueden modificarse para evitar la inspección. Consulte Dirección IP reenviada para obtener más información y las prácticas recomendadas.

Instancias y recuentos de agregación de reglas basados en tasas

Cuando una regla basada en tasas evalúa las solicitudes web utilizando sus criterios de agregación, cada conjunto único de valores que la regla encuentra para las claves de agregación especificadas define una instancia de agregación única.

- Varias claves: si ha definido varias claves personalizadas, el valor de cada clave contribuye a la definición de la instancia de agregación. Cada combinación única de valores define una instancia de agregación.
- Clave única: si ha elegido una clave única, ya sea en las claves personalizadas o seleccionando una de las opciones de dirección IP única, cada valor único de la clave define una instancia de agregación.
- Contar todas, sin claves: si ha seleccionado la opción de agregación Contar todas, todas las solicitudes que la regla evalúe pertenecerán a una sola instancia de agregación de la regla. Esta opción requiere una instrucción de restricción de acceso.

Una regla basada en tasas cuenta las solicitudes web por separado para cada instancia de agregación que identifica.

Por ejemplo, supongamos que una regla basada en tasas evalúa las solicitudes web con los siguientes valores de dirección IP y método HTTP:

- Dirección IP 10.1.1.1, método HTTP POST
- Dirección IP 10.1.1.1, método HTTP GET

- Dirección IP 127.0.0.0, método HTTP POST
- Dirección IP 10.1.1.1, método HTTP GET

La regla crea distintas instancias de agregación según sus criterios de agregación.

- Si el criterio de agregación es solo la dirección IP, cada dirección IP individual es una instancia de agregación y AWS WAF cuenta las solicitudes por separado para cada una. Las instancias de agregación y los recuentos de solicitudes de nuestro ejemplo serían los siguientes:
  - Dirección IP 10.1.1.1: recuento 3
  - Dirección IP 127.0.0.0: recuento 1
- Si el criterio de agregación es el método HTTP, cada método HTTP individual es una instancia de agregación. Las instancias de agregación y los recuentos de solicitudes de nuestro ejemplo serían los siguientes:
  - Método HTTP POST: recuento 2
  - Método HTTP GET: recuento 2
- Si los criterios de agregación son la dirección IP y el método HTTP, cada dirección IP y cada método HTTP contribuirían a la instancia de agregación combinada. Las instancias de agregación y los recuentos de solicitudes de nuestro ejemplo serían los siguientes:
  - Dirección IP 10.1.1.1, método HTTP POST: recuento 1
  - Dirección IP 10.1.1.1, método HTTP GET: recuento 2
  - Dirección IP 127.0.0.0, método HTTP POST: recuento 1

Comportamiento de limitación de velocidad de solicitud de reglas basadas en la tasa

El criterio que se AWS WAF utiliza para limitar las solicitudes de una regla basada en tasas es el mismo que se AWS WAF utiliza para agregar las solicitudes de la regla. Si define una declaración de alcance reducido para la regla, AWS WAF solo agrega, cuenta y limita las solicitudes que coincidan con la declaración de alcance reducido.

Los criterios de coincidencia que hacen que una regla basada en tasas aplique su configuración de acción de regla a una solicitud web específica son los siguientes:

- La solicitud web coincide con la instrucción de restricción de acceso de la regla, si se ha definido alguna.

- La solicitud web pertenece a una instancia de agregación cuyo recuento de solicitudes supera actualmente el límite de la regla.

AWS WAF ¿Cómo se aplica la acción de la regla?

Cuando una regla basada en la tasa aplica un límite de velocidad a una solicitud, aplica la acción de la regla y, si has definido algún tratamiento o etiquetado personalizados en la especificación de la acción, la regla los aplica. Esta gestión de solicitudes es la misma que la forma en que una regla de coincidencia aplica su configuración de acciones a las solicitudes web coincidentes. Una regla basada en tasas solo aplica etiquetas o realiza otras acciones a las solicitudes cuya tasa está limitando activamente.

Puede utilizar cualquier acción de regla excepto Allow. Para obtener información general sobre las acciones de las reglas, consulte Acción de regla.

La siguiente lista describe cómo funciona la limitación de velocidad para cada una de las acciones.

- Block— AWS WAF bloquea la solicitud y aplica cualquier comportamiento de bloqueo personalizado que hayas definido.
- Count— AWS WAF cuenta la solicitud, aplica los encabezados o etiquetas personalizados que haya definido y continúa con la evaluación web de la solicitud mediante ACL.

  Esta acción no limita la tasa de solicitudes. Solo cuenta las solicitudes que superan el límite.
- CAPTCHA o Challenge: AWS WAF gestiona la solicitud como Block o como Count, según el estado del token de la solicitud.

  Esta acción no limita la cantidad de solicitudes que tienen tokens válidos. Limita el número de solicitudes que sobrepasan el límite y a las que también les faltan fichas válidas.

  - Si la solicitud no tiene un token válido y vigente, la acción bloquea la solicitud y envía al cliente el rompecabezas de CAPTCHA o el desafío del navegador.

    Si el navegador del usuario final o del cliente responde correctamente, el cliente recibe un token válido y reenvía automáticamente la solicitud original. Si el límite de velocidad para la instancia de agregación sigue en vigor, a esta nueva solicitud con el token válido y vigente se le aplicará la acción que se describe en el siguiente punto.
  - Si la solicitud tiene un token válido y vigente, la acción CAPTCHA o Challenge verifica el token y no realiza ninguna acción a la solicitud, similar a la acción Count. La regla basada en la tasa

devuelve la evaluación de la solicitud a la ACL web sin tomar ninguna medida de finalización, y la ACL web continúa evaluando la solicitud.

Para obtener información adicional, consulte CAPTCHAy Challenge en AWS WAF.

Si limita la tasa solo a la dirección IP o la dirección IP reenviada

Al configurar la regla para limitar la tasa únicamente a la dirección IP reenviada, la instancia de la regla puede limitar la tasa hasta a 10 000 direcciones IP. Si una instancia de regla identifica más de 10 000 direcciones IP para limitar la tasa, solo limita los 10 000 remitentes más altos.

Con esta configuración, puede recuperar la lista de direcciones IP cuya velocidad está limitando actualmente una regla basada en la velocidad. Si utilizas una declaración de alcance, las solicitudes que tienen una velocidad limitada son solo las de la lista de IP que coinciden con la declaración de alcance. Para obtener información sobre cómo recuperar la lista de direcciones IP, consulte Lista de direcciones IP cuyas tasas están limitada por reglas basadas en tasas.

Ejemplos de reglas basadas en tasas

En esta sección, se describen ejemplos de configuraciones para diversos casos de uso comunes de reglas basadas en tasas.

Cada ejemplo proporciona una descripción del caso de uso y, a continuación, muestra la solución en las listas JSON para las reglas configuradas de forma personalizada.

> **Note**
>
> Las listas JSON que se muestran en estos ejemplos se crearon en la consola configurando la regla y, a continuación, editándola con el Editor de reglas JSON.

Temas

- Limitación de las tasas de las solicitudes a una página de inicio de sesión
- Limitación de las tasas de las solicitudes a una página de inicio de sesión desde cualquier par de agente de usuario y dirección IP
- Limitación de la tasas de las solicitudes a las que les falta un encabezado específico
- Limitación de las tasas de las solicitudes con etiquetas específicas

- Limitación de las tasas de las solicitudes de etiquetas que tienen un espacio de nombres de etiquetas específico

Limitación de las tasas de las solicitudes a una página de inicio de sesión

Para limitar el número de solicitudes a la página de inicio de sesión de su sitio web sin que ello afecte al tráfico al resto del sitio, puede crear una regla basada en tasas con una instrucción de restricción de acceso que haga coincidir las solicitudes con la página de inicio de sesión y con la agregación de solicitudes establecida en Contar todas.

La regla basada en tasas contará todas las solicitudes de la página de inicio de sesión en una sola instancia de agregación y aplicará la acción de regla cuando las solicitudes superen el límite.

En la siguiente lista de JSON, se muestra un ejemplo de esta configuración de reglas. La opción de agregación de contar todas aparece en JSON como configuración `CONSTANT`. En este ejemplo, la coincidencia es con las páginas de inicio de sesión que comienzan con `/login`.

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 1000,
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CONSTANT",
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
```

```
              "Type": "NONE",
              "Priority": 0
            }
          ]
        }
      }
    }
  }
}
```

Limitación de las tasas de las solicitudes a una página de inicio de sesión desde cualquier par de agente de usuario y dirección IP

Para limitar el número de solicitudes a la página de inicio de sesión de su sitio web para pares de agente de usuario y dirección IP que superen su límite, defina la agregación de solicitudes en Claves personalizadas y especifique los criterios de agregación.

En la siguiente lista de JSON, se muestra un ejemplo de esta configuración de reglas. En este ejemplo, hemos establecido el límite en 100 solicitudes en un período de cinco minutos por par de direcciones IP y agentes de usuario.

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CUSTOM_KEYS",
      "CustomKeys": [
        {
          "Header": {
            "Name": "User-Agent",
            "TextTransformations": [
```

```
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        },
        {
          "IP": {}
        }
      ],
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
              "Type": "NONE",
              "Priority": 0
            }
          ]
        }
      }
    }
  }
}
```

Limitación de la tasas de las solicitudes a las que les falta un encabezado específico

Para limitar el número de solicitudes a las que les falta un encabezado específico, puede usar la opción de agregación Contar todas con una instrucción de restricción de acceso. Configure la instrucción de restricción de acceso con una instrucción lógica `NOT` que contenga una instrucción que demuestre ser verdadera solo si el encabezado existe y tiene un valor.

En la siguiente lista de JSON, se muestra un ejemplo de esta configuración de reglas.

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
```

```
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 1000,
      "AggregateKeyType": "CONSTANT",
      "EvaluationWindowSec": 300,
      "ScopeDownStatement": {
        "NotStatement": {
          "Statement": {
            "SizeConstraintStatement": {
              "FieldToMatch": {
                "SingleHeader": {
                  "Name": "user-agent"
                }
              },
              "ComparisonOperator": "GT",
              "Size": 0,
              "TextTransformations": [
                {
                  "Type": "NONE",
                  "Priority": 0
                }
              ]
            }
          }
        }
      }
    }
  }
}
```

Limitación de las tasas de las solicitudes con etiquetas específicas

Puede combinar la limitación de tasas con cualquier regla o grupo de reglas que añada etiquetas a las solicitudes para limitar el número de solicitudes de diferentes categorías. Para ello, configure su ACL web de la siguiente manera:

- Agregue las reglas o los grupos de reglas que agregan etiquetas y configúrelos para que no bloqueen ni permitan las solicitudes cuya tasa desea limitar. Si usa grupos de reglas administrados, es posible que deba anular algunas acciones de regla de los grupos de reglas Count para lograr este comportamiento.
- Agregue una regla basada en tasas a su ACL web con una configuración de número de prioridad superior a la de las reglas de etiquetado y los grupos de reglas. AWS WAF evalúa las reglas en orden numérico, empezando por el más bajo, de modo que la regla basada en tasas se ejecute después de las reglas de etiquetado. Configure el límite de tasas en las etiquetas mediante una combinación de concordancia de etiquetas en la instrucción de restricción de acceso y agregación de etiquetas de la regla.

En el siguiente ejemplo, se utiliza el grupo de reglas de reglas AWS gestionadas de la lista de reputaciones IP de Amazon. La regla `AWSManagedIPDDoSList` del grupo de reglas detecta y etiqueta las solicitudes cuyas IP se sabe que participan activamente en actividades de DDoS. La acción de regla está configurada en Count en la definición del grupo de reglas. Para obtener más información acerca de este grupo de reglas, consulte the section called “Lista de reputación de IP de Amazon”.

La siguiente lista de JSON de ACL web utiliza el grupo de reglas de reputación de IP seguido de una regla basada en tasas de coincidencia de etiquetas. La regla basada en tasas utiliza una instrucción de restricción de acceso para filtrar las solicitudes que han sido marcadas por la regla del grupo de reglas. La instrucción de regla basada en tasas agrega y limita las tasas de las solicitudes filtradas por sus direcciones IP.

```
{
  "Name": "test-web-acl",
  "Id": ...
  "ARN": ...
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesAmazonIpReputationList",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
```

```
          "Name": "AWSManagedRulesAmazonIpReputationList"
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesAmazonIpReputationList"
      }
    },
    {
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 100,
          "EvaluationWindowSec": 300,
          "AggregateKeyType": "IP",
          "ScopeDownStatement": {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList"
            }
          }
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "test-rbr"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
  },
  "Capacity": 28,
```

```
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}
```

Limitación de las tasas de las solicitudes de etiquetas que tienen un espacio de nombres de etiquetas específico

Las reglas de nivel común del grupo de reglas administrado de control de bots agregan etiquetas para bots de distintas categorías, pero solo bloquean las solicitudes de bots no verificados. Para obtener información acerca de estas reglas, consulte Listado de reglas de control de bots.

Si utiliza el grupo de reglas administrado de control de bots, puede agregar un límite de tasas para las solicitudes de bots verificados individuales. Para ello, añada una regla basada en tasas que se ejecute después del grupo de reglas de control de bots y agregue las solicitudes por las etiquetas de los nombres de los bots. Especifique la clave de agregación del Espacio de nombres de la etiqueta y establezca la clave del espacio de nombres en `awswaf:managed:aws:bot-control:bot:name:`. Cada etiqueta única con el espacio de nombres especificado definirá una instancia de agregación. Por ejemplo, las etiquetas `awswaf:managed:aws:bot-control:bot:name:axios` y `awswaf:managed:aws:bot-control:bot:name:curl` definen una instancia de agregación.

En la siguiente lista JSON de ACL, se muestra un ejemplo de esta configuración de reglas. La regla de este ejemplo limita las solicitudes de cualquier instancia de agregación de bots a 1000 en un período de dos minutos.

```
{
  "Name": "test-web-acl",
  "Id": ...
  "ARN": ...
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesBotControlRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesBotControlRuleSet",
```

```
        "ManagedRuleGroupConfigs": [
          {
            "AWSManagedRulesBotControlRuleSet": {
              "InspectionLevel": "COMMON"
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesBotControlRuleSet"
    }
  },
  {
    "Name": "test-rbr",
    "Priority": 1,
    "Statement": {
      "RateBasedStatement": {
        "Limit": 1000,
        "EvaluationWindowSec": 120,
        "AggregateKeyType": "CUSTOM_KEYS",
        "CustomKeys": [
          {
            "LabelNamespace": {
              "Namespace": "awswaf:managed:aws:bot-control:bot:name:"
            }
          }
        ]
      }
    },
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "test-rbr"
    }
  }
```

```
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
  },
  "Capacity": 82,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}
```

Lista de direcciones IP cuyas tasas están limitada por reglas basadas en tasas

Si la regla basada en la velocidad solo agrega la dirección IP o la dirección IP reenviada, puede recuperar la lista de direcciones IP cuya velocidad está limitando actualmente la regla. AWS WAF almacena estas direcciones IP en la lista de claves administradas de la regla.

> **Note**
>
> Esta opción solo está disponible si se agrega solo la dirección IP o solo una dirección IP de un encabezado. Si utiliza la agregación de solicitudes de claves personalizadas, no podrá recuperar una lista de direcciones IP con tasas limitadas, aunque utilice una de las especificaciones de direcciones IP en sus claves personalizadas.

Una regla basada en tasas aplica su acción de regla a las solicitudes de la lista de claves administradas de la regla que coinciden con la instrucción de restricción de acceso de la regla. Cuando una regla no tiene una instrucción de restricción de acceso, aplica la acción a todas las solicitudes de las direcciones IP que figuran en la lista. La acción de regla es Block de forma predeterminada, pero puede ser cualquier acción de regla válida excepto Allow. El número máximo de direcciones IP que AWS WAF pueden limitar la velocidad mediante una única instancia de regla basada en la velocidad es de 10 000. Si más de 10 000 direcciones superan el límite de velocidad, AWS WAF limita las que tengan las tasas más altas.

Puede acceder a la lista de claves administradas de una regla basada en tasas mediante la CLI, la API o cualquier SDK. En este tema se aborda el acceso mediante la CLI y las API. La consola no proporciona acceso a la lista en este momento.

Para la AWS WAF API, el comando es GetRateBasedStatementManagedKeys.

Para la AWS WAF CLI, el comando es get-rate-based-statement-managed-keys.

A continuación, se muestra la sintaxis para recuperar la lista de direcciones IP de velocidad limitada para una regla basada en la velocidad que se utiliza en una ACL web en una distribución de Amazon CloudFront .

```
aws wafv2 get-rate-based-statement-managed-keys --scope=CLOUDFRONT --region=us-east-1
 --web-acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

A continuación, se muestra la sintaxis de una aplicación regional, una API REST de Amazon API Gateway, una Application Load Balancer, una API de AWS AppSync GraphQL, un grupo de usuarios de Amazon Cognito, un AWS App Runner servicio o una instancia de acceso verificado. AWS

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-
acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

AWS WAF supervisa las solicitudes web y administra las claves de forma independiente para cada combinación única de ACL web, grupo de reglas opcional y regla basada en tasas. Por ejemplo, si define una regla basada en tasas dentro de un grupo de reglas y, a continuación, usa el grupo de reglas en una ACL web, AWS WAF monitoriza las solicitudes web y administra las claves de esa ACL web, instrucción de referencia del grupo de reglas e instancia de regla basada en tasas. Si usa el mismo grupo de reglas en una segunda ACL web, AWS WAF supervisa las solicitudes web y administra las claves para este segundo uso con total independencia del primero.

Para una regla basada en tasas que haya definido dentro de un grupo de reglas, debe proporcionar el nombre de la instrucción de referencia del grupo de reglas en su solicitud, además del nombre de la ACL web y el nombre de la regla basada en tasas dentro del grupo de reglas. A continuación, se muestra la sintaxis de una aplicación regional en la que la regla basada en tasas se define dentro de un grupo de reglas y el grupo de reglas se usa en una ACL web.

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-
acl-name=WebACLName --web-acl-id=WebACLId --rule-group-rule-name=RuleGroupRuleName --
rule-name=RuleName
```

Instrucciones de regla de grupos de reglas

Las instrucciones de regla de los grupos de reglas no se pueden anidar.

En esta sección, se describen las instrucciones de regla de los grupos de reglas que puede usar en su ACL web. Las unidades de capacidad de ACL web (WCU) del grupo de reglas las establece el propietario del grupo de reglas en el momento de la creación. Para obtener información acerca de las WCU, consulte AWS WAF unidades de capacidad ACL web (WCU).

Instrucción de grupo de reglas	Descripción	WCU
Grupo de reglas administrado	Ejecuta las reglas definidas en el grupo de reglas administr ado especificado. Puede reducir el alcance de las solicitudes que evalúa el grupo de reglas agregando una instrucción de restricción de acceso. No puede anidar una instrucci ón de grupo de reglas administrado dentro de una instrucción de otro tipo.	Definido por el grupo de reglas, más cualquier WCU adicional para una instrucción de restricción de acceso.
Grupo de reglas	Ejecuta las reglas definidas en un grupo de reglas que administra. No puede agregar una instrucción de restricción de acceso a una instrucción de referencia del grupo de reglas para su propio grupo de reglas. No puede anidar una instrucci ón de grupo de reglas dentro de una instrucción de otro tipo	Defina el límite de WCU para el grupo de reglas al crearlo.

Instrucción de grupo de reglas administrado

La instrucción de regla de grupo de reglas administrado añade una referencia de la lista de reglas de la ACL web a un grupo de reglas administrado. No aparece esta opción en las instrucciones de reglas de la consola. Sin embargo, cuando se trabaja con el formato JSON de la ACL web, los grupos de reglas administrados que haya agregado aparecen en las reglas de la ACL web con este tipo.

Un grupo de reglas administrado puede ser un grupo de reglas AWS administradas, la mayoría de las cuales son gratuitas para AWS WAF los clientes, o un grupo de reglas AWS Marketplace administradas. Los grupos de reglas de pago de AWS Managed Rules se suscriben automáticamente al añadirlos a la ACL web. Puede suscribirse a los grupos de reglas AWS Marketplace gestionados a través de AWS Marketplace. Para obtener más información, consulte Grupos de reglas administrados.

Al agregar un grupo de reglas a una ACL web, puede anular las acciones de las reglas del grupo de reglas para Count o para otra acción de la regla. Para obtener más información, consulte Opciones de anulación de acciones para grupos de reglas.

Puede reducir el alcance de las solicitudes que se AWS WAF evalúan con el grupo de reglas. Para ello, debe agregar una instrucción de restricción de acceso dentro de la instrucción del grupo de reglas. Para obtener información sobre las instrucciones de restricción de acceso, consulte Instrucciones de restricción de acceso. Esto puede ayudarle a gestionar la forma en que el grupo de reglas afecta al tráfico y puede ayudarle a contener los costos asociados al volumen de tráfico cuando utiliza el grupo de reglas. Para obtener información y ejemplos sobre el uso de sentencias de alcance reducido con el grupo de reglas gestionado por AWS WAF Bot Control, consulte. AWS WAF Control de bots

No se puede anidar: no se puede anidar este tipo de instrucción en otras instrucciones y no se puede incluir en ningún grupo de reglas. Puede incluirlo directamente en una ACL web.

(Opcional) Instrucción de restricción de acceso: este tipo de regla utiliza una instrucción de restricción de acceso opcional para restringir el acceso de las solicitudes que evalúa el grupo de reglas. Para obtener más información, consulte Instrucciones de restricción de acceso.

WCU: se establecen para el grupo de reglas cuando se crean.

Dónde encontrar esta instrucción de regla

- Consola: durante el proceso de creación de una ACL web, en la página Añadir reglas y grupos de reglas, elija Añadir grupos de reglas administrados y, a continuación, busque y seleccione el grupo de reglas que desea usar.
- API: ManagedRuleGroupStatement

Instrucción de grupo de reglas

La instrucción de regla de grupo de reglas añade una referencia de la lista de reglas de la ACL web a un grupo de reglas que administra. No aparece esta opción en las instrucciones de reglas de la consola. Sin embargo, cuando se trabaja con el formato JSON de la ACL web, cualquier grupo de reglas administrado que haya agregado aparece en las reglas de la ACL web con este tipo. Para obtener información acerca de sus propios grupos de reglas, consulte Administrar sus propios grupos de reglas.

Al agregar un grupo de reglas a una ACL web, puede anular las acciones de las reglas del grupo de reglas para Count o para otra acción de la regla. Para obtener más información, consulte Opciones de anulación de acciones para grupos de reglas.

No se puede anidar: no se puede anidar este tipo de instrucción en otras instrucciones y no se puede incluir en ningún grupo de reglas. Puede incluirlo directamente en una ACL web.

WCU: se establecen para el grupo de reglas cuando se crean.

Dónde encontrar esta instrucción de regla

- Consola: durante el proceso de creación de una ACL web, en la página Añadir reglas y grupos de reglas, elija Añadir mis propias reglas y grupos de reglas), Grupo de reglas y, a continuación, agregue el grupo de reglas que desea usar.
- API — RuleGroupReferenceStatement

Manejo de componentes de solicitudes sobredimensionadas en AWS WAF

AWS WAF no admite la inspección de contenidos muy grandes para el cuerpo, los encabezados o las cookies de los componentes de las solicitudes web. El servicio de alojamiento subyacente tiene límites de recuento y tamaño en cuanto a lo que reenvía para AWS WAF su inspección. Por

ejemplo, el servicio de alojamiento no envía más de 200 encabezados, por lo que AWS WAF, en el caso de una solicitud web con 205 encabezados, no AWS WAF puede inspeccionar los últimos 5 encabezados.

Cuando se AWS WAF permite que una solicitud web pase a tu recurso protegido, se envía la solicitud web completa, incluido el contenido que se encuentra fuera de los límites de recuento y tamaño que AWS WAF se pudieron inspeccionar.

Límites de tamaño de inspección de componentes

Los límites de tamaño de inspección de los componentes son los siguientes:

- **`Body`**y **`JSON Body`** — Para Application Load Balancer y AWS AppSync, AWS WAF puede inspeccionar los primeros 8 KB del cuerpo de una solicitud. Para CloudFront API Gateway, Amazon Cognito, App Runner y Verified Access, de forma predeterminada, AWS WAF pueden inspeccionar los primeros 16 KB y usted puede aumentar el límite hasta 64 KB en su configuración de ACL web. Para obtener más información, consulte Gestión de los límites de tamaño de la inspección corporal.
- **`Headers`**— AWS WAF puede inspeccionar como máximo los primeros 8 KB (8.192 bytes) de los encabezados de las solicitudes y, como máximo, los primeros 200 encabezados. El contenido está disponible para su inspección AWS WAF hasta que se alcance el primer límite.
- **`Cookies`**— AWS WAF puede inspeccionar como máximo los primeros 8 KB (8.192 bytes) de las cookies solicitadas y, como máximo, las 200 primeras cookies. El contenido está disponible para su inspección AWS WAF hasta que se alcance el primer límite.

Opciones de gestión del sobredimensionamiento para sus instrucciones de reglas

Cuando escriba una instrucción de regla que inspecciona uno de estos tipos de componentes de solicitud, especifique cómo gestionar los componentes sobredimensionados. El manejo del tamaño excesivo indica AWS WAF qué hacer con una solicitud web cuando el componente de la solicitud que la regla inspecciona supera los límites de tamaño.

Las opciones de gestión de componentes sobredimensionados son las siguientes:

- Continue— Inspeccione el componente de la solicitud normalmente de acuerdo con los criterios de inspección de la regla. AWS WAF inspeccionará el contenido del componente solicitado que se encuentre dentro de los límites de tamaño.
- Match— Considera que la solicitud web coincide con el enunciado 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.

- 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 ACL web, como lo haría con cualquier regla que no coincida.

En la AWS WAF consola, debes elegir una de estas opciones de gestión. Fuera de la consola, la opción predeterminada es Continue.

Si utiliza la opción Match en una regla cuya acción esté establecida en Block, la regla bloqueará una solicitud cuyo componente inspeccionado esté sobredimensionado. Con cualquier otra configuración, la disposición final de la solicitud depende de varios factores, como la configuración de las demás reglas de la ACL web y la configuración de acción predeterminada de la ACL web.

Gestión de sobredimensionamiento en grupos de reglas que no le pertenecen

Las limitaciones de tamaño y número de componentes se aplican a todas las reglas que utilice en su ACL web. Esto incluye todas las reglas que utilice pero no administre en los grupos de reglas administrados y en los grupos de reglas que otra cuenta comparta con usted.

Cuando utilice un grupo de reglas que no administre, es posible que el grupo de reglas tenga una regla que inspeccione un componente de solicitud limitado, pero que no gestione el contenido sobredimensionado de la forma en que necesita que se gestione. Para obtener información sobre cómo las reglas AWS administradas administran los componentes de gran tamaño, consulteAWS Lista de grupos de reglas de Managed Rules. Para obtener información sobre otros grupos de reglas, pregunte a su proveedor de grupos de reglas.

Directrices para administrar componentes sobredimensionados en su ACL web

La forma en que gestione los componentes sobredimensionados en su ACL web puede depender de varios factores, como el tamaño esperado del contenido de los componentes de la solicitud, la gestión predeterminada de las solicitudes por parte de la ACL web y la forma en que otras reglas de su ACL web establecen coincidencias y gestionan las solicitudes.

Las pautas generales para administrar los componentes sobredimensionados de solicitudes web son las siguientes:

- Si necesita permitir algunas solicitudes con un contenido de componentes sobredimensionados, si es posible, añada reglas para permitir explícitamente solo esas solicitudes. Priorice esas reglas para que se ejecuten antes que cualquier otra regla de la ACL web que inspeccione los mismos

tipos de componentes. Con este enfoque, no podrá AWS WAF inspeccionar todo el contenido de los componentes sobredimensionados que permite pasar a su recurso protegido.

- Para todas las demás solicitudes, puede evitar que pasen bytes adicionales bloqueando las solicitudes que superen el límite:
  - Sus reglas y grupos de reglas: en las reglas que inspeccionan los componentes con límites de tamaño, configure la gestión del sobredimensionamiento para bloquear las solicitudes que superen el límite. Por ejemplo, si su regla bloquea las solicitudes con un contenido de encabezado específico, configure la gestión del sobredimensionamiento para que coincida con las solicitudes que tienen un contenido de encabezado sobredimensionado. Como alternativa, si su ACL web bloquea las solicitudes de forma predeterminada y su regla permite un contenido de encabezado específico, configure la gestión del sobredimensionamiento de la regla para que no coincida con ninguna solicitud que tenga un contenido de encabezado sobredimensionado.
  - Grupos de reglas que no administra: para evitar que los grupos de reglas que no administra permitan componentes de solicitudes sobredimensionados, puede agregar una regla independiente que inspeccione el tipo de componente de solicitud y bloquee las solicitudes que sobrepasen los límites. Dé prioridad a la regla en su ACL web para que se ejecute antes de los grupos de reglas. Por ejemplo, puede bloquear las solicitudes con un contenido de cuerpo sobredimensionado antes de que alguna de sus reglas de inspección del cuerpo se ejecute en la ACL web. El siguiente procedimiento describe cómo agregar este tipo de regla.

Bloquear componentes de solicitudes web sobredimensionados

Puede agregar una regla en su ACL web que bloquee las solicitudes con componentes sobredimensionados.

Cómo agregar una regla que bloquee el contenido sobredimensionado

1. Al crear o editar su ACL web, en la configuración de reglas, elija Agregar reglas, Agregar mis propias reglas y grupos de reglas, Generador de reglas y, a continuación, Editor visual de reglas. Para obtener información sobre cómo crear o editar una ACL web, consulte Trabajar con ACL web.
2. Introduzca un nombre para la regla y deje la opción Tipo en Regla normal.
3. Cambia las siguientes configuraciones de coincidencia de sus valores predeterminados:

   a. En Instrucción, en Inspeccionar, abra el menú desplegable y elija el componente de solicitud web que necesite: Cuerpo, Encabezados o Cookies.

b. En Tipo de coincidencia, seleccione Tamaño mayor que.

c. En Tamaño, escriba un número que sea al menos el tamaño mínimo para el tipo de componente. Para los encabezados y las cookies, escriba. `8192` En Application Load Balancer o ACL AWS AppSync web, para cuerpos, escriba. `8192` Para los cuerpos que se encuentren en CloudFront las ACL web de API Gateway, Amazon Cognito, App Runner o Verified Access, si utiliza el límite de tamaño corporal predeterminado, escriba. `16384` De lo contrario, escriba el límite de tamaño corporal que ha definido para su ACL web.

d. Para Gestionar sobredimensionamiento, seleccione Coincidencia.

4. En Acción, seleccione Bloquear.
5. Seleccione Agregar regla.
6. Tras agregar la regla, en la página Establecer la prioridad de la regla, colóquela por encima de cualquier regla o grupo de reglas de la ACL web que inspeccione el mismo tipo de componente. Esto le da a la nueva regla una configuración de prioridad numérica más baja, lo que hace AWS WAF que la evalúe primero. Para obtener más información, consulte Procesamiento del orden de las reglas y los grupos de reglas en una ACL web.

Coincidencia de patrones de expresiones regulares en AWS WAF

AWS WAF admite la sintaxis de patrones utilizada por la biblioteca `libpcre` PCRE. La biblioteca está documentada en PCRE, expresiones regulares compatibles con Perl.

AWS WAF no es compatible con todas las construcciones de la biblioteca. Por ejemplo, admite algunas afirmaciones de ancho cero, pero no todas. No tenemos una lista completa de los constructos compatibles. Sin embargo, si proporcionas un patrón de expresiones regulares que no es válido o utilizas construcciones no compatibles, la AWS WAF API informa de un error.

AWS WAF no admite los siguientes patrones de PCRE:

- Referencias a elementos anteriores y subexpresiones de captura
- Referencias de subrutinas y patrones recursivos
- Patrones condicionales
- Verbos de control de búsqueda de datos anteriores
- La directiva \C de byte único
- La directiva \R de coincidencia de nueva línea
- El inicio \K de la directiva de restablecimiento de coincidencia

- Llamadas y código incrustado
- Cuantificadores atómicos de agrupamiento y posesivos

Conjuntos de IP y conjuntos de patrones de expresiones regulares en AWS WAF

AWS WAF almacena información más compleja en conjuntos que usted utiliza haciendo referencia a ellos en sus reglas. Cada uno de estos conjuntos tiene un nombre. A cada conjunto se le asigna un nombre de recurso de Amazon (ARN) en el momento de su creación. Puede administrar estos conjuntos desde el interior de las instrucciones de regla y puede acceder a ellos y administrarlos por separado mediante el panel de navegación de la consola.

Puede usar un conjunto administrado en un grupo de reglas o en una ACL web.

- Para usar un conjunto de direcciones IP, consulteInstrucción de regla de coincidencia de conjuntos de IP.
- Para utilizar un conjunto de patrones de expresiones regulares, consulte. Instrucción de regla de coincidencia de conjuntos de patrones de regex

Incoherencias temporales durante las actualizaciones

Al crear o cambiar una ACL web u otros AWS WAF recursos, los cambios tardan un poco en propagarse a todas las áreas donde se almacenan los recursos. El tiempo de propagación puede oscilar entre unos segundos y varios minutos.

A continuación, se proporcionan ejemplos de incoherencias temporales que podría notar durante la propagación de los cambios:

- Después de crear una ACL web, si intenta asociarla a un recurso, es posible que se produzca una excepción que indique que la ACL web no está disponible.
- Después de agregar un grupo de reglas a una ACL web, las nuevas reglas del grupo de reglas pueden estar en vigor en un área en la que se usa la ACL web y no en otra.
- Tras cambiar la configuración de una acción de regla, es posible que vea la acción anterior en algunos lugares y la acción nueva en otros.
- Después de agregar una dirección IP a un conjunto de IP que está en uso dentro de una regla de bloqueo, es posible que la nueva dirección se bloquee en un área, pero que se permita en otra.

Temas

Crear y administrar un conjunto de IP

Un conjunto de IP proporciona una recopilación de las direcciones IP y rangos de direcciones IP que desea utilizar juntos en una instrucción de regla. Los conjuntos de IP son AWS recursos.

Para usar un conjunto de IP en una ACL web o en un grupo de reglas, primero debe crear un AWS recurso `IPSet` con las especificaciones de su dirección. A continuación, tiene que hacer referencia al conjunto al agregar la instrucción de regla de un conjunto de IP a una ACL web o a un grupo de reglas.

Temas

Crear un conjunto de IP

Siga el procedimiento de esta sección para crear un nuevo conjunto de IP.

> **Note**
>
> Además del procedimiento descrito en esta sección, tiene la opción de agregar un nuevo conjunto de IP al agregar una regla de coincidencia de IP a su ACL web o grupo de reglas. Decantarse por esa opción requiere proporcionar la misma configuración necesaria para este procedimiento.

Para crear un conjunto de IP

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, elija IP sets (Conjuntos de IP) y, a continuación, Create IP Set (Crear conjunto de IP).

3. Introduzca un nombre y la descripción del conjunto de IP. Los usará para identificar el conjunto cuando desee usarlo.

   > **Note**
   >
   > No se puede cambiar el nombre después de crear el conjunto.

4. En Región, elija Global (CloudFront) o elija la región en la que desee almacenar el conjunto de IP. Puede usar conjuntos de IP regionales solo en las ACL web que protegen los recursos regionales. Para usar una IP establecida en las ACL web que protegen CloudFront las distribuciones de Amazon, debes usar Global ()CloudFront.
5. En el caso de IP version (versión de IP), seleccione la versión que desee utilizar.
6. En el cuadro de texto de direcciones IP, introduzca una dirección IP o un intervalo de direcciones IP por línea, en notación CIDR. AWS WAF admite todos los rangos CIDR de IPv4 e IPv6 excepto. `/0` Para obtener más información acerca de la notación CIDR, consulte el artículo de Wikipedia Classless Inter-Domain Routing.

   Estos son algunos ejemplos:

   - Para especificar la dirección IPv4 192.0.2.44, escriba 192.0.2.44/32.
   - Para especificar la dirección de IPv6 2620:0:2d0:200:0:0:0:0, escriba 2620:0:2d0:200:0:0:0:0/128.
   - Para especificar el rango de direcciones IPv4 de 192.0.2.0 a 192.0.2.255, escriba 192.0.2.0/24.
   - Para especificar el rango de direcciones IPv6 de 2620:0:2d0:200:0:0:0:0 a 2620:0:2d0:200:ffff:ffff:ffff:ffff, introduzca 2620:0:2d0:200::/64.
7. Revise la configuración del conjunto de IP y seleccione Create IP set (Crear conjunto de IP).

Eliminar un conjunto de IP

Siga las instrucciones que se detallan en esta sección para eliminar un conjunto al que se haga referencia.

Eliminación de conjuntos o grupos de reglas al que se hace referencia

Al eliminar una entidad que puede usar en una ACL web, como un conjunto de IP, un conjunto de patrones de expresiones regulares o un grupo de reglas, AWS WAF comprueba si la entidad se está

utilizando actualmente en una ACL web. Si descubre que está en uso, AWS WAF le avisa. AWS WAF casi siempre puede determinar si una ACL web está haciendo referencia a una entidad. No obstante, es posible que en algunos casos no consiga hacerlo. Si tiene que asegurarse de que no hay nada que esté utilizando actualmente la entidad, verifique sus ACL de la web antes de eliminarla. Si la entidad es un conjunto al que se hace referencia, verifique que ningún grupo de reglas la esté utilizando.

Para eliminar un conjunto de IP

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, elija IP sets (Conjuntos de IP).
3. Seleccione el conjunto de IP que desee eliminar y seleccione Delete (Eliminar).

Crear y administrar un conjunto de patrones de expresiones regex

Un conjunto de patrones de expresiones regex proporciona una recopilación de las expresiones regex que desea utilizar juntas en una instrucción de regla. Los conjuntos de patrones de expresiones regulares son AWS recursos.

Para usar un conjunto de patrones de expresiones regulares en una ACL web o un grupo de reglas, primero debe crear un AWS recurso `RegexPatternSet` con las especificaciones del patrón de expresiones regulares. A continuación, tiene que hacer referencia al conjunto al agregar la instrucción de regla a un conjunto de patrones de expresiones regex a una ACL web o a un grupo de reglas. Un conjunto de patrones de especificaciones regex debe contener al menos un patrón de especificaciones regex.

Si el conjunto de expresiones regulares contiene más de un patrón, la coincidencia de patrones se combina con una lógica `OR`. Es decir, una solicitud web coincidirá con la instrucción de regla del conjunto si el componente de la solicitud coincide con cualquiera de los patrones del conjunto.

AWS WAF admite la sintaxis de patrones utilizada por la biblioteca PCRE, con algunas excepciones. `libpcre` La biblioteca está documentada en PCRE, expresiones regulares compatibles con Perl. Para obtener información sobre el AWS WAF soporte, consulteCoincidencia de patrones de expresiones regulares en AWS WAF.

Temas

- Crear un conjunto de patrones de expresiones regex

- Eliminar un conjunto de patrones de expresiones regex

Crear un conjunto de patrones de expresiones regex

Siga el procedimiento de esta sección para crear un nuevo conjunto de patrones de expresiones regex.

Para crear un conjunto de patrones de expresiones regex

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, elija Regex pattern sets (Conjuntos de patrones de expresiones regex) y, a continuación, Create regex pattern set (Crear conjunto de patrones de expresiones regex).
3. Introduzca un nombre y una descripción para el conjunto de patrones de expresiones regex. Los usará para identificar el conjunto cuando desee usarlo.

   > **Note**
   >
   > No se puede cambiar el nombre después de crear el conjunto.

4. En Región, selecciona Global (CloudFront) o elige la región en la que deseas almacenar el conjunto de patrones de expresiones regulares. Puede usar conjuntos de expresiones regulares regionales solo en las ACL web que protegen los recursos regionales. Para usar un patrón de expresiones regulares establecido en las ACL web que protegen CloudFront las distribuciones de Amazon, debes usar Global (). CloudFront
5. En el cuadro de texto Regular expressions (Expresiones regulares), introduzca un patrón de expresiones regex por línea.

   Por ejemplo, la expresión regular `I[a@]mAB[a@]dRequest` concuerda con las siguientes cadenas: `IamABadRequest`, `IamAB@dRequest`, `I@mABadRequest` y `I@mAB@dRequest`.

   AWS WAF admite la sintaxis de patrones utilizada por la biblioteca PCRE con algunas excepciones. `libpcre` La biblioteca está documentada en PCRE, expresiones regulares compatibles con Perl. Para obtener información sobre el AWS WAF soporte, consulteCoincidencia de patrones de expresiones regulares en AWS WAF.

6. Revise la configuración del conjunto de patrones de expresiones regulares y elija Create regex pattern set (Crear conjunto de patrones de expresiones regex).

Eliminar un conjunto de patrones de expresiones regex

Siga las instrucciones que se detallan en esta sección para eliminar un conjunto al que se haga referencia.

Eliminación de conjuntos o grupos de reglas al que se hace referencia

Al eliminar una entidad que puede usar en una ACL web, como un conjunto de IP, un conjunto de patrones de expresiones regulares o un grupo de reglas, AWS WAF comprueba si la entidad se está utilizando actualmente en una ACL web. Si descubre que está en uso, AWS WAF le avisa. AWS WAF casi siempre puede determinar si una ACL web está haciendo referencia a una entidad. No obstante, es posible que en algunos casos no consiga hacerlo. Si tiene que asegurarse de que no hay nada que esté utilizando actualmente la entidad, verifique sus ACL de la web antes de eliminarla. Si la entidad es un conjunto al que se hace referencia, verifique que ningún grupo de reglas la esté utilizando.

Para eliminar un conjunto de patrones de expresiones regex

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, elija Regex pattern sets (Conjuntos de patrones de expresiones regex).
3. Seleccione el conjunto que desee eliminar y haga clic en Delete (Eliminar).

Solicitudes web y respuestas personalizadas en AWS WAF

Puede añadir un comportamiento personalizado de gestión de solicitudes y respuestas web a sus acciones de AWS WAF regla y a las acciones de ACL web predeterminadas. La configuración personalizada se aplica siempre que se aplique la acción a la que está asociada.

Puede personalizar las solicitudes web y las respuestas de las siguientes maneras:

- Con las acciones Allow, Count, CAPTCHA y Challenge, puede insertar encabezados personalizados en la solicitud web. Cuando AWS WAF reenvía la solicitud web al recurso protegido, la solicitud contiene toda la solicitud original más los encabezados personalizados

que haya insertado. Para las acciones CAPTCHA y Challenge, AWS WAF solo aplica la personalización si la solicitud pasa la inspección del CAPTCHA o del token de desafío.

- Con las acciones Block, puede definir una respuesta personalizada completa, con código de respuesta, encabezados y cuerpo. El recurso protegido responde a la solicitud mediante la respuesta personalizada proporcionada por AWS WAF. Su respuesta personalizada reemplaza la respuesta de acción predeterminada Block de `403 (Forbidden)`.

Configuraciones de acción personalizables

Puede especificar una solicitud o respuesta personalizadas al definir las siguientes configuraciones de acción:

- Acción de la regla. Para obtener más información, consulte Acción de regla.
- Acción predeterminada para la ACL web. Para obtener más información, consulte La acción predeterminada de ACL web.

Configuraciones de acción puede personalizar

No puede especificar una gestión de solicitudes personalizada en la acción de anulación de un grupo de reglas que utilice en una ACL web. Consulte Evaluación de reglas y grupos de reglas de ACL web. Consulte también Instrucción de grupo de reglas administrado y Instrucción de grupo de reglas.

Incoherencias temporales durante las actualizaciones

Al crear o cambiar una ACL web u otros AWS WAF recursos, los cambios tardan un poco en propagarse a todas las áreas donde se almacenan los recursos. El tiempo de propagación puede oscilar entre unos segundos y varios minutos.

A continuación, se proporcionan ejemplos de incoherencias temporales que podría notar durante la propagación de los cambios:

- Después de crear una ACL web, si intenta asociarla a un recurso, es posible que se produzca una excepción que indique que la ACL web no está disponible.
- Después de agregar un grupo de reglas a una ACL web, las nuevas reglas del grupo de reglas pueden estar en vigor en un área en la que se usa la ACL web y no en otra.
- Tras cambiar la configuración de una acción de regla, es posible que vea la acción anterior en algunos lugares y la acción nueva en otros.

- Después de agregar una dirección IP a un conjunto de IP que está en uso dentro de una regla de bloqueo, es posible que la nueva dirección se bloquee en un área, pero que se permita en otra.

Limita el uso de solicitudes y respuestas personalizadas

AWS WAF define la configuración máxima para el uso de solicitudes y respuestas personalizadas. Por ejemplo, un número máximo de encabezados de solicitud por ACL web o grupo de reglas, y un número máximo de encabezados personalizados para una única definición de respuesta personalizada. Para obtener más información, consulte AWS WAF cuotas.

Temas

- Inserciones de encabezados de solicitud personalizados para acciones no bloqueantes
- Respuestas personalizadas para las acciones Block
- Códigos de estado compatibles para la respuesta personalizada

Inserciones de encabezados de solicitud personalizados para acciones no bloqueantes

Puedes indicar que AWS WAF insertes encabezados personalizados en la solicitud HTTP original cuando una acción de regla no bloquee la solicitud. Con esta opción, solo agrega a la solicitud. No puede modificar ni reemplazar ninguna parte de la solicitud original. Los casos de uso para la inserción de encabezados personalizados incluyen indicar a una aplicación posterior que procese la solicitud de forma diferente en función de los encabezados insertados y marcar la solicitud para su análisis.

Esta opción se aplica a las acciones de regla Allow, Count, CAPTCHA y Challenge, y a las acciones predeterminadas de la ACL web configuradas en Allow. Para obtener más información sobre las acciones de las reglas, consulte Acción de regla. Para obtener más información acerca de las acciones ACL web predeterminadas, consulte La acción predeterminada de ACL web.

Nombres de encabezados de solicitud personalizados

AWS WAF pone prefijos a todos los encabezados de solicitud con los que inserta`x-amzn-waf-`, para evitar confusiones con los encabezados que ya están en la solicitud. Por ejemplo, si especificas el nombre del encabezado`sample`, AWS WAF inserta el encabezado. `x-amzn-waf-sample`

Encabezados con el mismo nombre

Si la solicitud ya tiene un encabezado con el mismo nombre que el que AWS WAF se está insertando, AWS WAF sobrescribe el encabezado. Por lo tanto, si define encabezados en varias reglas con nombres idénticos, se agregará su encabezado a la última regla que inspeccione la solicitud y encuentre una coincidencia, y no a las reglas anteriores.

Encabezados personalizados con acciones de regla de no de finalización

A diferencia de la Allow acción, la Count acción no detiene el procesamiento AWS WAF de la solicitud web mediante el resto de las reglas de la ACL web. Del mismo modo, cuando se CAPTCHA Challenge determina que el token de solicitud es válido, estas acciones no AWS WAF impiden procesar la solicitud web. Por lo tanto, si inserta encabezados personalizados mediante una regla con una de estas acciones, es posible que las reglas subsiguientes también inserten encabezados personalizados. Para obtener más información sobre el comportamiento de las acciones de las reglas, consulte Acción de regla.

Por ejemplo, supongamos que tiene las reglas siguientes, priorizadas en el orden que se muestra:

1. RuleA con una acción Count y un encabezado personalizado denominado `RuleAHeader`.
2. RuleB con una acción Allow y un encabezado personalizado denominado `RuleBHeader`.

Si una solicitud coincide con la regla A y la regla B, AWS WAF inserta los encabezados `x-amzn-waf-RuleAHeader` y`x-amzn-waf-RuleBHeader`, a continuación, reenvía la solicitud al recurso protegido.

AWS WAF inserta encabezados personalizados en una solicitud web cuando termina de inspeccionarla. Por lo tanto, si utiliza una gestión de solicitudes personalizadas con una regla que tenga la acción establecida en Count, las siguientes reglas no inspeccionarán los encabezados personalizados que añada.

Ejemplo de gestión de solicitudes personalizadas

La gestión de solicitudes personalizadas se define para la acción de una regla o para la acción predeterminada de una ACL web. En la siguiente lista se muestra la JSON para la gestión personalizada agregada a la acción predeterminada de una ACL web.

```
{
 "Name": "SampleWebACL",
 "Scope": "REGIONAL",
 "DefaultAction": {
  "Allow": {
```

```
   "CustomRequestHandling": {
    "InsertHeaders": [
     {
      "Name": "fruit",
      "Value": "watermelon"
     },
     {
      "Name": "pie",
      "Value": "apple"
     }
    ]
   }
  }
 },
 "Description": "Sample web ACL with custom request handling configured for default
 action.",
 "Rules": [],
 "VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "SampleWebACL"
 }
}
```

Respuestas personalizadas para las acciones Block

Puede indicar que envíe una respuesta HTTP personalizada AWS WAF al cliente para las acciones de regla o las acciones predeterminadas de ACL web que estén configuradas en. Block Para obtener más información sobre las acciones de las reglas, consulte Acción de regla. Para obtener más información acerca de las acciones ACL web predeterminadas, consulte La acción predeterminada de ACL web.

Al definir la gestión de respuestas personalizadas para una acción Block, define el código de estado, los encabezados y el cuerpo de la respuesta. Para obtener una lista de los códigos de estado con los que puede AWS WAF utilizarlos, consulte la sección siguiente:. Códigos de estado compatibles para la respuesta personalizada

Casos de uso

Entre los casos de uso de respuestas personalizadas se incluyen los siguientes:

- Envío de un código de estado no predeterminado de vuelta al cliente.

- Devolver encabezados de respuesta personalizada al cliente. Puede especificar cualquier nombre de encabezamiento salvo para el `content-type`.
- Envío una página de error estática al cliente.
- Redireccionamiento del cliente a una URL diferente. Para ello, especifique uno de los códigos de estado de redirección de `3xx`, como `301 (Moved Permanently)` o `302 (Found)`, y, a continuación, especifique un nuevo encabezado con el nombre `Location` y con la nueva URL.

Interacción con las respuestas que defina en su recurso protegido

Las respuestas personalizadas que especifique para la AWS WAF Block acción tienen prioridad sobre cualquier especificación de respuesta que defina en el recurso protegido.

El servicio de alojamiento del AWS recurso con el que se protege AWS WAF puede permitir la gestión personalizada de las respuestas para las solicitudes web. Algunos ejemplos son los siguientes:

- Con Amazon CloudFront, puedes personalizar la página de error en función del código de estado. Para obtener más información, consulta Generar respuestas de error personalizadas en la Guía para CloudFront desarrolladores de Amazon.
- Con Amazon API Gateway, puede definir el código de respuesta y estado de su puerta de enlace. Para obtener información, consulte el tema Respuestas de la puerta de enlace en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

No puede combinar la configuración de respuesta AWS WAF personalizada con la configuración de respuesta personalizada en el AWS recurso protegido. La especificación de respuesta para cualquier solicitud web individual proviene completamente de AWS WAF o completamente del recurso protegido.

En el caso de las solicitudes web que AWS WAF bloquean, a continuación se muestra el orden de prioridad.

1. AWS WAF respuesta personalizada: si la AWS WAF Block acción tiene habilitada una respuesta personalizada, el recurso protegido devuelve la respuesta personalizada configurada al cliente. Cualquier configuración de respuesta que haya definido en el propio recurso protegido no tiene ningún efecto.

2. Respuesta personalizada definida en el recurso protegido: de lo contrario, si el recurso protegido tiene una configuración de respuesta personalizada especificada, el recurso protegido utiliza esa configuración para responder al cliente.
3. AWS WAF Blockrespuesta predeterminada: de lo contrario, el recurso protegido responde al cliente con la Block respuesta AWS WAF predeterminada`403 (Forbidden)`.

En el caso de las solicitudes web que lo AWS WAF permitan, la configuración del recurso protegido determina la respuesta que envía al cliente. No puedes configurar los ajustes de respuesta AWS WAF para las solicitudes permitidas. La única personalización que puedes configurar AWS WAF para las solicitudes permitidas es la inserción de encabezados personalizados en la solicitud original antes de reenviarla al recurso protegido. Esta opción se ha descrito en la sección anterior, Inserciones de encabezados de solicitud personalizados para acciones no bloqueantes.

Encabezados de respuesta personalizados

Puede especificar cualquier nombre de encabezamiento salvo para el `content-type`.

Cuerpos de respuesta personalizados

El cuerpo de una respuesta personalizada se define en el contexto de la ACL web o del grupo de reglas en el que desee utilizarla. Una vez que haya definido un cuerpo de respuesta personalizado, puede usarlo como referencia en cualquier otro lugar de la ACL web o del grupo de reglas en el que lo creó. En la configuración de la acción individual Block, se hace referencia al cuerpo personalizado que se quiere usar y se definen el código de estado y el encabezado de la respuesta personalizada.

Cuando crea una respuesta personalizada en la consola, puede elegir entre los cuerpos de respuesta que ya ha definido o puede crear un nuevo cuerpo. Fuera de la consola, puede definir los cuerpos de respuesta personalizados en la ACL web o en el grupo de reglas, y, a continuación, hacer referencia a ellos desde la configuración de las acciones de la ACL web o del grupo de reglas. Esto se muestra en el ejemplo JSON de la siguiente sección.

Respuesta personalizada de ejemplo

En el siguiente ejemplo, se muestra la JSON de un grupo de reglas con una configuración de respuesta personalizada. El cuerpo de la respuesta personalizada se define para todo el grupo de reglas y, a continuación, se hace referencia a él mediante una clave en la acción de regla.

```
{
 "ARN": "test_rulegroup_arn",
 "Capacity": 1,
```

```
"CustomResponseBodies": {
 "CustomResponseBodyKey1": {
  "Content": "This is a plain text response body.",
  "ContentType": "TEXT_PLAIN"
 }
},

"Description": "This is a test rule group.",
"Id": "test_rulegroup_id",
"Name": "TestRuleGroup",

"Rules": [
 {
  "Action": {
   "Block": {
    "CustomResponse": {
     "CustomResponseBodyKey": "CustomResponseBodyKey1",
     "ResponseCode": 404,
     "ResponseHeaders": [
      {
       "Name": "BlockActionHeader1Name",
       "Value": "BlockActionHeader1Value"
      }
     ]
    }
   }
  },
  "Name": "GeoMatchRule",
  "Priority": 1,
  "Statement": {
   "GeoMatchStatement": {
    "CountryCodes": [
     "US"
    ]
   }
  },
  "VisibilityConfig": {
   "CloudWatchMetricsEnabled": true,
   "MetricName": "TestRuleGroupReferenceMetric",
   "SampledRequestsEnabled": true
  }
 }
],
```

```
  "VisibilityConfig": {
   "CloudWatchMetricsEnabled": true,
   "MetricName": "TestRuleGroupMetric",
   "SampledRequestsEnabled": true
  }
 }
```

Códigos de estado compatibles para la respuesta personalizada

Para obtener información detallada sobre los códigos de estado HTTP, consulte Códigos de estado del Grupo de Trabajo de Ingeniería de Internet (IETF) y la Lista de códigos de estado HTTP en Wikipedia.

Los siguientes son los códigos de estado HTTP que AWS WAF admiten las respuestas personalizadas.

- 2xx Successful
  - 200 – OK
  - 201 – Created
  - 202 – Accepted
  - 204 – No Content
  - 206 – Partial Content
- 3xx Redirection
  - 300 – Multiple Choices
  - 301 – Moved Permanently
  - 302 – Found
  - 303 –See Other
  - 304 – Not Modified
  - 307 – Temporary Redirect
  - 308 – Permanent Redirect
- 4xx Client Error
  - 400 – Bad Request
  - 401 – Unauthorized
  - 403 – Forbidden
  - 404 – Not Found

  - 405 – Method Not Allowed
  - 408 – Request Timeout
  - 409 – Conflict
  - 411 – Length Required
  - 412 – Precondition Failed
  - 413 – Request Entity Too Large
  - 414 – Request-URI Too Long
  - 415 – Unsupported Media Type
  - 416 – Requested Range Not Satisfiable
  - 421 – Misdirected Request
  - 429 – Too Many Requests
- 5xx Server Error
  - 500 – Internal Server Error
  - 501 – Not Implemented
  - 502 – Bad Gateway
  - 503 – Service Unavailable
  - 504 – Gateway Timeout
  - 505 – HTTP Version Not Supported

AWS WAF etiquetas en las solicitudes web

Una etiqueta es un metadato que una regla añade a una solicitud web cuando la regla coincide con la solicitud. Una vez agregada, la etiqueta permanece disponible en la solicitud hasta que finalice la evaluación de la ACL web. Puede acceder a las etiquetas de las reglas que se ejecutan más adelante en la evaluación de la ACL web mediante una instrucción de coincidencia de etiquetas. Para obtener más detalles, consulte Instrucción de regla de coincidencia de etiquetas.

Las etiquetas de las solicitudes web generan métricas de CloudWatch etiquetas de Amazon. Para ver una lista de las métricas y dimensiones, consulte Etiquetar métricas y dimensiones. Para obtener información sobre cómo acceder a las métricas CloudWatch y a los resúmenes de métricas a través de la AWS WAF consola, consulteMonitorización y ajuste.

Casos de uso del etiquetado

Entre los casos de uso habituales de AWS WAF las etiquetas se incluyen los siguientes:

- Evaluación de una solicitud web comparándola con varias sentencias de reglas antes de tomar medidas con respecto a la solicitud: después de encontrar una coincidencia con una regla en una ACL web, AWS WAF continúa evaluando la solicitud en función de la ACL web si la acción de la regla no finaliza la evaluación de la ACL web. Puede usar etiquetas para evaluar y recopilar información de varias reglas antes de decidir permitir o bloquear la solicitud. Para ello, cambie las acciones de reglas existentes a Count y configúrelas para que añadan etiquetas a las solicitudes coincidentes. A continuación, agregue una o más reglas nuevas para que se ejecuten después del resto de reglas, y configúrelas para evaluar las etiquetas y administrar las solicitudes de acuerdo con las combinaciones de coincidencias de etiquetas.
- Administración de las solicitudes web por región geográfica: puede usar solo la regla de coincidencia geográfica para administrar las solicitudes web por país de origen. Para ajustar la ubicación en cuanto a la región, se utiliza la regla de coincidencia geográfica con una acción Count seguida de una regla de coincidencia de etiquetas. Para obtener información sobre la regla de coincidencia geográfica, consulte Instrucción de regla de coincidencia geográfica.
- Reutilización de la lógica en varias reglas: si necesita reutilizar la misma lógica en varias reglas, puede usar etiquetas para obtener la lógica de una sola fuente y comprobar los resultados. Cuando tiene varias reglas complejas que utilizan un subconjunto común de instrucciones de reglas anidadas, duplicar el conjunto de reglas común en todas las reglas complejas puede llevar mucho tiempo y llevar a errores. Con las etiquetas, puede crear una nueva regla con el subconjunto de reglas común que cuenta las solicitudes coincidentes y les agrega una etiqueta. Agregue la nueva regla a su ACL web para que se ejecute antes que las complejas reglas originales. A continuación, en las reglas originales, se reemplaza el subconjunto de reglas compartidas por una sola regla que comprueba la etiqueta.

  Por ejemplo, supongamos que tiene varias reglas que desea aplicar únicamente a sus rutas de inicio de sesión. En lugar de hacer que cada regla especifique la misma lógica para que coincida con las posibles rutas de inicio de sesión, puede implementar una sola regla nueva que contenga esa lógica. Haga que la nueva regla añada una etiqueta a las solicitudes coincidentes para indicar que la solicitud se encuentra en una ruta de inicio de sesión. En su ACL web, asigne a esta nueva regla una prioridad numérica inferior a la de las reglas originales para que se ejecute primero. A continuación, en las reglas originales, sustituya la lógica compartida por una comprobación de la presencia de la etiqueta. Para obtener información acerca de la configuración de prioridad, consulte Procesamiento del orden de las reglas y los grupos de reglas en una ACL web.
- Creación de excepciones a las reglas en los grupos de reglas: esta opción resulta especialmente útil para los grupos de reglas administrados, que no se pueden ver ni modificar. Muchas reglas

de grupos de reglas administrados agregan etiquetas a las solicitudes web coincidentes para indicar las reglas que coinciden y, posiblemente, para proporcionar información adicional sobre la coincidencia. Cuando usa un grupo de reglas que agrega etiquetas a las solicitudes, puede anular las reglas del grupo de reglas para contar las coincidencias y, a continuación, ejecutar una regla después del grupo de reglas que gestiona la solicitud web en función de las etiquetas del grupo de reglas. Todas las reglas administradas de AWS agregan etiquetas a las solicitudes web coincidentes. Para ver los detalles, consulte las descripciones de las reglas en AWS Lista de grupos de reglas de Managed Rules.

- Uso de métricas de etiquetas para supervisar los patrones de tráfico: puede acceder a las métricas de las etiquetas que añada a través de sus reglas y a las métricas agregadas por cualquier grupo de reglas administrado que utilice en su ACL web. Todos los grupos de reglas administrados AWS agregan etiquetas a las solicitudes web que evalúan. Para ver una lista de las métricas y dimensiones de las etiquetas, consulte Etiquetar métricas y dimensiones. Puede acceder a las métricas y a los resúmenes de métricas a través CloudWatch de la página web de ACL de la AWS WAF consola. Para obtener más información, consulte Monitorización y ajuste.

Cómo funciona el AWS WAF etiquetado

Cuando una regla coincide con una solicitud web, si la regla tiene etiquetas definidas, AWS WAF agrega las etiquetas a la solicitud al final de la evaluación de la regla. Las reglas que se evalúan después de la regla de coincidencia en la ACL web pueden coincidir con las etiquetas que la regla ha agregado.

Quién añade etiquetas a las solicitudes

Los componentes de la ACL web que evalúan las solicitudes pueden agregar etiquetas a las solicitudes.

- Cualquier regla que no sea una instrucción de referencia de un grupo de reglas puede agregar etiquetas a las solicitudes web coincidentes. Los criterios de etiquetado forman parte de la definición de la regla y, cuando una solicitud web coincide con la regla, AWS WAF agrega las etiquetas de la regla a la solicitud. Para obtener más información, consulte the section called “Reglas que añaden etiquetas”.
- La instrucción de la regla de coincidencia geográfica agrega etiquetas de país y región a todas las solicitudes que inspecciona, independientemente de si encuentra o no una coincidencia. Para obtener más información, consulte the section called “Coincidencia geográfica”.

- Las reglas AWS gestionadas para AWS WAF todos añaden etiquetas a las solicitudes que inspeccionan. Agregan algunas etiquetas en función de las coincidencias de reglas en el grupo de reglas y otras en función de los procesos de AWS que utilizan los grupos de reglas administrados, como el etiquetado de token que se agrega cuando se usa un grupo de reglas de mitigación de amenazas inteligente. Para obtener información sobre las etiquetas que agrega cada grupo de reglas administrado, consulte the section called “AWS Lista de grupos de reglas de Managed Rules”.

¿Cómo AWS WAF gestiona las etiquetas

AWS WAF agrega las etiquetas de la regla a la solicitud al final de la inspección de la solicitud por parte de la regla. El etiquetado forma parte de las actividades de coincidencia de una regla, de forma similar a la acción.

Las etiquetas no persisten en la solicitud web una vez finalizada la evaluación de la ACL web. Para que otras reglas coincidan con una etiqueta que agregue su regla, la acción de regla no debe finalizar la evaluación de la solicitud web por parte de la ACL web. La acción de regla debe estar establecida en Count, CAPTCHA, o Challenge. Cuando la evaluación de la ACL web no finaliza, las reglas posteriores de la ACL web pueden ejecutar sus criterios de coincidencia de etiquetas con la solicitud. Para obtener más información sobre las acciones de las reglas, consulte Acción de regla.

Acceso a las etiquetas durante la evaluación de la ACL web

Una vez agregadas, las etiquetas permanecen disponibles en la solicitud siempre que AWS WAF se evalúe la solicitud con respecto a la ACL web. Cualquier regla de una ACL web puede acceder a las etiquetas que han agregado las reglas que ya se han ejecutado en la misma ACL web. Esto incluye las reglas que se definen directamente en la ACL web y las reglas definidas dentro de los grupos de reglas que se utilizan en la ACL web.

- Para hacer coincidir los criterios de inspección de la solicitud de la regla con una etiqueta, utilice la instrucción de concordancia de etiquetas. Puede compararla con cualquier etiqueta que se adjunte a la solicitud. Para obtener información detallada sobre la instrucción, consulte Instrucción de regla de coincidencia de etiquetas.
- La instrucción de coincidencia geográfica agrega etiquetas con o sin coincidencia, pero solo están disponibles después de que la instrucción que contiene la regla de ACL web haya completado la evaluación de la solicitud.
  - No puede usar una sola regla, por ejemplo, una instrucción lógica `AND`, para ejecutar una instrucción de concordancia geográfica seguida de una instrucción de concordancia de etiquetas

con las etiquetas geográficas. Debe colocar la instrucción de coincidencia de etiquetas en una regla independiente que se ejecute después de la regla que contiene la instrucción de coincidencia geográfica.

- Si utiliza una instrucción de coincidencia geográfica como una instrucción de restricción de acceso dentro de una instrucción de regla basada en tasas o una instrucción de referencia de un grupo de reglas administrado, las etiquetas que agrega la instrucción de coincidencia geográfica no están disponibles para que las inspeccione la instrucción de la regla contenedora. Si necesita inspeccionar el etiquetado geográfico en una instrucción de regla basada en tasas o en un grupo de reglas, debe ejecutar la instrucción de coincidencia geográfica en una regla independiente que se ejecute de antemano.

Acceso a la información de las etiquetas fuera de la evaluación web de la ACL

Las etiquetas no persisten con la solicitud web una vez finalizada la evaluación de la ACL web, sino que AWS WAF registra la información de las etiquetas en los registros y en las métricas.

- AWS WAF almacena las CloudWatch estadísticas de Amazon de las primeras 100 etiquetas de una sola solicitud. Para obtener información sobre cómo obtener acceso a las métricas de etiquetas, consulte Monitorización con Amazon CloudWatch y Etiquetar métricas y dimensiones.
- AWS WAF resume las métricas de las CloudWatch etiquetas en los paneles de información general del tráfico de ACL web de la AWS WAF consola. Puede acceder a los paneles de control desde cualquier página de la ACL web. Para obtener más información, consulte Paneles de información general sobre el tráfico de ACL web.
- AWS WAF registra las etiquetas en los registros para las 100 primeras etiquetas de una solicitud. Puede usar etiquetas, junto con la acción de regla, para filtrar los registros que registra AWS WAF . Para obtener más información, consulte Registro del tráfico de ACL AWS WAF web.

Su evaluación de ACL web puede aplicar más de 100 etiquetas a una solicitud web y compararlas con más de 100 etiquetas, pero AWS WAF solo registra las 100 primeras de los registros y las métricas.

AWS WAF requisitos de nomenclatura y sintaxis de etiquetas

Una etiqueta es una cadena compuesta de un prefijo, espacios de nombres opcionales y un nombre. Los componentes de una etiqueta se delimitan con dos puntos. Las etiquetas tienen los siguientes requisitos y características:

- Las etiquetas distinguen entre mayúsculas y minúsculas.
- Cada espacio de nombres o nombre de etiqueta puede tener hasta 128 caracteres.
- Puede especificar hasta cinco espacios de nombres en una etiqueta.
- Los componentes de una etiqueta están separados por dos puntos (`:`).
- No puede usar las siguientes cadenas reservadas en los espacios de nombres o en el nombre que especifique para una etiqueta: `awswaf`, `aws`, `waf`, `rulegroup`, `webacl`, `regexpatternset`, `ipset` y `managed`.

Sintaxis de etiquetas

Una etiqueta completa tiene un prefijo, espacios de nombres opcionales y un nombre de etiqueta. El prefijo identifica el grupo de reglas o el contexto de ACL web de la regla que agregó la etiqueta. Los espacios de nombres se pueden usar para agregar más contexto a la etiqueta. El nombre de la etiqueta proporciona el nivel de detalle más bajo para una etiqueta. Suele indicar la regla específica que ha agregado la etiqueta a la solicitud.

El prefijo de la etiqueta varía según su origen.

- Sus etiquetas: a continuación, se muestra la sintaxis completa de las etiquetas que cree en la ACL web y en las reglas de los grupos de reglas. Los tipos de entidad son `rulegroup` y `webacl`.

  ```
  awswaf:<entity owner account id>:<entity type>:<entity name>:<custom
   namespace>:...:<label name>
  ```

  - Prefijo del espacio de nombres de la etiqueta: `awswaf:<entity owner account id>:<entity type>:<entity name>:`
  - Adiciones de espacios de nombres personalizados: `<custom namespace>:…:`

  Al definir una etiqueta para una regla en un grupo de reglas o una ACL web, se controlan las cadenas de espacio de nombres personalizadas y el nombre de la etiqueta. El resto lo genera para usted AWS WAF. AWS WAF pone automáticamente como prefijo a todas las etiquetas la configuración de la cuenta y de la ACL web o de la entidad del grupo de reglas. `awswaf`

- Etiquetas de grupos de reglas administrados: a continuación, se muestra la sintaxis completa de las etiquetas que crean las reglas de los grupos de reglas administrados.

  ```
  awswaf:managed:<vendor>:<rule group name>:<custom namespace>:...:<label name>
  ```

  - Prefijo del espacio de nombres de la etiqueta: `awswaf:managed:<vendor>:<rule group name>:`
  - Adiciones de espacios de nombres personalizados: `<custom namespace>:…:`

  Todos los grupos de reglas de AWS Managed Rules añaden etiquetas. Para obtener información acerca de los grupos de reglas administrados, consulte Grupos de reglas administrados.

- Etiquetas de otros AWS procesos: los grupos de reglas de reglas AWS administradas utilizan estos procesos, por lo que se agregan a las solicitudes web que se evalúan mediante grupos de reglas administrados. A continuación, se muestra la sintaxis completa de las etiquetas que crean los procesos a los que llaman los grupos de reglas administrados.

  ```
  awswaf:managed:<process>:<custom namespace>:...:<label name>
  ```

  - Prefijo del espacio de nombres de la etiqueta: `awswaf:managed:<process>:`
  - Adiciones de espacios de nombres personalizados: `<custom namespace>:…:`

  Se muestran etiquetas de este tipo para los grupos de reglas administrados que llaman al proceso de AWS . Para obtener información acerca de los grupos de reglas administrados, consulte Grupos de reglas administrados.

Ejemplos de etiquetas para sus reglas

Los siguientes ejemplos de etiquetas se definen mediante reglas de un grupo de reglas denominado `testRules` que pertenece a la cuenta, 111122223333.

```
awswaf:111122223333:rulegroup:testRules:testNS1:testNS2:LabelNameA
```

```
awswaf:111122223333:rulegroup:testRules:testNS1:LabelNameQ
```

```
awswaf:111122223333:rulegroup:testRules:LabelNameZ
```

En la siguiente lista se muestra un ejemplo de especificación de etiqueta en JSON. Estos nombres de etiquetas incluyen cadenas de espacios de nombres personalizadas antes del nombre final de la etiqueta.

```
Rule: {
    Name: "label_rule",
```

```
    Statement: {...}
    RuleLabels: [
        Name: "header:encoding:utf8",
        Name: "header:user_agent:firefox"
    ],
    Action: { Count: {} }
}
```

> **Note**
>
> Puede acceder a este tipo de listado en la consola a través del editor de reglas JSON.

Si ejecuta la regla anterior en el mismo grupo de reglas y en la misma cuenta que en los ejemplos de etiquetas anteriores, las etiquetas completas resultantes serían las siguientes:

```
awswaf:111122223333:rulegroup:testRules:header:encoding:utf8
```

```
awswaf:111122223333:rulegroup:testRules:header:user_agent:firefox
```

Ejemplos de etiquetas para grupos de reglas administrados

A continuación, se muestran ejemplos de etiquetas de los grupos de reglas de AWS Managed Rules y los procesos que invocan.

```
awswaf:managed:aws:core-rule-set:NoUserAgent_Header
```

```
awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments
```

```
awswaf:managed:aws:atp:aggregate:attribute:compromised_credentials
```

```
awswaf:managed:token:accepted
```

AWS WAF reglas que añaden etiquetas

En casi todas las reglas, puedes definir etiquetas y AWS WAF aplicarlas a cualquier solicitud coincidente.

Los siguientes tipos de reglas son las únicas excepciones:

- Las reglas basadas en la tasa solo etiquetan mientras limitan la velocidad: las reglas basadas en la tasa solo agregan etiquetas a las solicitudes web de una instancia de agregación específica mientras esa instancia tiene una velocidad limitada. AWS WAF Para obtener información acerca de las reglas basadas en tasas, consulte Instrucción de regla basada en frecuencia.
- No se permite etiquetar en las declaraciones de referencia de los grupos de reglas: la consola no acepta etiquetas para estos tipos de reglas. A través de la API, si se especifica una etiqueta para cualquier tipo de declaración, se produce una excepción de validación. Para obtener información sobre estos tipos de instrucciones, consulte Instrucción de grupo de reglas administrado y Instrucción de grupo de reglas.

WCU: 1 WCU por cada 5 etiquetas que defina en su ACL web o en las reglas del grupo de reglas.

Dónde encontrarlo

- Creador de reglas de la consola: en la configuración Acción de la regla, en Etiqueta.
- Tipo de datos de la API: `Rule` `RuleLabels`

Para definir una etiqueta en una regla, especifique las cadenas de espacio de nombres personalizadas y el nombre que se van a añadir al prefijo del espacio de nombres de la etiqueta. AWS WAF deriva el prefijo del contexto en el que se define la regla. Para obtener más información al respecto, consulte la información sobre la sintaxis de la etiqueta que aparece en AWS WAF requisitos de nomenclatura y sintaxis de etiquetas.

AWS WAF reglas que coinciden con las etiquetas

Puede usar una instrucción de coincidencia de etiquetas para evaluar las etiquetas de las solicitudes web. Puede compararla con Etiqueta, que requiere el nombre de la etiqueta, o con Espacio de nombres, que requiere una especificación de espacio de nombres. Tanto para la etiqueta como para el espacio de nombres, puede incluir opcionalmente los espacios de nombres anteriores y el prefijo en la especificación. Para obtener más información sobre esta instrucción de política, consulte Instrucción de regla de coincidencia de etiquetas.

El prefijo de una etiqueta define el contexto del grupo de reglas o ACL web donde se define la regla de la etiqueta. En la sentencia de coincidencia de etiquetas de una regla, si la cadena de coincidencia de etiquetas o espacios de nombres no especifica el prefijo, AWS WAF utiliza el prefijo para la regla de coincidencia de etiquetas.

- Las etiquetas de las reglas que se definen directamente dentro de una ACL web tienen un prefijo que especifica el contexto de la ACL web.
- Las etiquetas de las reglas que están dentro de un grupo de reglas tienen un prefijo que especifica el contexto del grupo de reglas. Puede ser su propio grupo de reglas o un grupo de reglas administrado por usted.

Para obtener más información al respecto, consulte la sintaxis de la etiqueta que aparece en AWS WAF requisitos de nomenclatura y sintaxis de etiquetas.

> **Note**
>
> Algunos grupos de reglas gestionados añaden etiquetas. Puede recuperarlos a través de la API llamando a `DescribeManagedRuleGroup`. Las etiquetas aparecen en la propiedad `AvailableLabels` de la respuesta.

Si quiere hacer coincidir una regla que se encuentra en un contexto diferente al contexto de su regla, debe proporcionar el prefijo en la cadena de coincidencia. Por ejemplo, si desea hacer coincidir las etiquetas que agregan las reglas de un grupo de reglas administrado, puede agregar una regla en su ACL web con una instrucción de coincidencia de etiqueta cuya cadena de coincidencia especifique el prefijo del grupo de reglas seguido de sus criterios de coincidencia adicionales.

En la cadena de coincidencia de la instrucción de coincidencia de etiquetas, especifique una etiqueta o un espacio de nombres:

- Etiqueta: la especificación de etiqueta de una coincidencia consiste en la parte final de la etiqueta. Puede incluir cualquier número de espacios de nombres contiguos que precedan inmediatamente al nombre de la etiqueta seguidos del nombre. También puede proporcionar la etiqueta completa empezando la especificación por el prefijo.

  Especificaciones de ejemplo:

  - `testNS1:testNS2:LabelNameA`
  - `awswaf:managed:aws:managed-rule-set:testNS1:testNS2:LabelNameA`
- Espacio de nombres: la especificación de espacio de nombres de una coincidencia consiste en cualquier subconjunto contiguo de la especificación de la etiqueta, excluido el nombre. Puede incluir el prefijo y puede incluir una o más cadenas de espacio de nombres.

Especificaciones de ejemplo:

- `testNS1:testNS2:`
- `awswaf:managed:aws:managed-rule-set:testNS1:`

AWS WAF ejemplos de concordancia de etiquetas

En esta sección se proporcionan ejemplos de especificaciones de coincidencia para la instrucción de la regla de coincidencia de etiquetas.

> **Note**
>
> Estas listas JSON se crearon en la consola añadiendo una regla a una ACL web con las especificaciones de coincidencia de etiquetas y, a continuación, editando la regla y cambiando al Editor de reglas JSON. También puede obtener el JSON de un grupo de reglas o ACL web a través de las API o de la interfaz de la línea de comandos.

Temas

Comparación con una etiqueta local

La siguiente lista de JSON muestra una instrucción de coincidencia de etiquetas para una etiqueta que se ha agregado a la solicitud web de forma local, en el mismo contexto que esta regla.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "header:encoding:utf8"
        }
```

```
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Si utiliza esta instrucción de coincidencia en la cuenta 111122223333, en una regla que defina para la ACL web `testWebACL`, coincidirá con las siguientes etiquetas.

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

```
awswaf:111122223333:webacl:testWebACL:testNS1:testNS2:header:encoding:utf8
```

No coincidiría con la siguiente etiqueta, porque la cadena de la etiqueta no coincide exactamente.

```
awswaf:111122223333:webacl:testWebACL:header:encoding2:utf8
```

No coincidiría con la siguiente etiqueta porque el contexto no es el mismo, por lo que el prefijo no coincide. Esto es cierto incluso si ha agregado el grupo de reglas `productionRules` a la ACL web `testWebACL`, donde se define la regla.

```
awswaf:111122223333:rulegroup:productionRules:header:encoding:utf8
```

Comparación con una etiqueta de otro contexto

La siguiente lista de JSON muestra una regla de coincidencia de etiquetas que coincide con una etiqueta de una regla de un grupo de reglas creado por el usuario. El prefijo es obligatorio en la especificación para todas las reglas que se ejecutan en la ACL web y que no forman parte del grupo de reglas mencionado. Esta especificación de etiqueta de ejemplo solo coincide con la etiqueta exacta.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:111122223333:rulegroup:testRules:header:encoding:utf8"
        }
    },
```

```
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Comparación con una etiqueta de grupo de reglas administrado

Este es un caso especial de coincidencia con una etiqueta que proviene de un contexto diferente al de la regla de coincidencia. La siguiente lista de JSON muestra una instrucción de coincidencia de etiquetas para una etiqueta de grupo de reglas administrado. Solo coincide con la etiqueta exacta que se especifica en la configuración clave de la instrucción de coincidencia de etiquetas.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:managed:aws:managed-rule-set:header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Comparación con un espacio de nombres local

La siguiente lista de JSON muestra una instrucción de coincidencia de etiquetas para un espacio de nombres local.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "NAMESPACE",
            Key: "header:encoding:"
        }
    },
    Labels: [
        ...generate_more_labels...
```

```
    ],
    Action: { Block: {} }
}
```

De forma similar a la coincidencia local `Label`, si usa esta instrucción en la cuenta 111122223333, en una regla que defina para la ACL web`testWebACL`, coincidirá con la siguiente etiqueta.

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

No coincidiría con la siguiente etiqueta porque la cuenta no es la misma, por lo que el prefijo no coincide.

```
awswaf:444455556666:webacl:testWebACL:header:encoding:utf8
```

El prefijo tampoco coincide con ninguna etiqueta aplicada por los grupos de reglas administrados, como las siguientes.

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

Comparación con un nombre de espacio de un grupo de reglas administrado

La siguiente lista de JSON muestra una instrucción de coincidencia de etiquetas para un espacio de nombres de grupo de reglas administrado. En el caso de un grupo de reglas de su propiedad, también tendrá que proporcionar el prefijo para que coincida con un espacio de nombres que esté fuera del contexto de la regla.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "NAMESPACE",
            Key: "awswaf:managed:aws:managed-rule-set:header:"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Esta especificación coincide con las siguientes etiquetas de ejemplo.

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

```
awswaf:managed:aws:managed-rule-set:header:encoding:unicode
```

No coincide con la siguiente etiqueta.

```
awswaf:managed:aws:managed-rule-set:query:badstring
```

AWS WAF mitigación inteligente de amenazas

En esta sección se describen las funciones gestionadas e inteligentes de mitigación de amenazas que ofrece. AWS WAF Se trata de protecciones avanzadas y especializadas que puede implementar para protegerse contra amenazas como los bots malintencionados y los intentos de apropiación de cuentas.

> **Note**
>
> Las funciones que se describen aquí conllevan costes adicionales, además de las tarifas básicas de uso AWS WAF. Para más información, consulte Precios de AWS WAF.

La orientación que se proporciona en esta sección está destinada a los usuarios que, en general, saben cómo crear y administrar las ACL, las reglas y los grupos de reglas AWS WAF web. Estos temas se tratan en secciones anteriores de esta guía.

Temas

- Opciones para la mitigación inteligente de amenazas
- Las prácticas recomendadas para la mitigación inteligente de amenazas
- AWS WAF tokens de solicitud web
- AWS WAF Control de fraude: creación de cuentas y prevención del fraude (ACFP)
- AWS WAF Control de fraudes y prevención de apropiación de cuentas (ATP)
- AWS WAF Control de bots
- AWS WAF integración de aplicaciones cliente

- CAPTCHAy Challenge en AWS WAF

Opciones para la mitigación inteligente de amenazas

En esta sección, se ofrece una comparación detallada de las opciones para implementar la mitigación de amenazas inteligentes.

AWS WAF ofrece los siguientes tipos de protecciones para la mitigación inteligente de amenazas.

- AWS WAF Control de fraudes y prevención del fraude en la creación de cuentas (ACFP): detecta y gestiona los intentos malintencionados de creación de cuentas en la página de registro de la aplicación. La funcionalidad principal la proporciona el grupo de reglas administrado de la ACFP. Para más información, consulte AWS WAF Control de fraude: creación de cuentas y prevención del fraude (ACFP) y AWS WAF Grupo de reglas de prevención del fraude (ACFP) para la creación de cuentas de Control de Fraude.
- AWS WAF Prevención del robo de cuentas (ATP) en Fraud Control: detecta y gestiona los intentos de apropiación maliciosos en la página de inicio de sesión de la aplicación. La funcionalidad principal la proporciona el grupo de reglas administrado de la ATP. Para más información, consulte AWS WAF Control de fraudes y prevención de apropiación de cuentas (ATP) y AWS WAF Grupo de reglas de prevención de apropiación de cuentas (ATP) para el control del fraude.
- AWS WAF Control de bots: identifica, etiqueta y gestiona tanto los bots amistosos como los maliciosos. Esta característica permite gestionar los bots habituales con firmas únicas en todas las aplicaciones, así como los bots objetivo que tienen firmas específicas para una aplicación. La funcionalidad principal la proporciona el grupo de reglas administrado de control de bots. Para más información, consulte AWS WAF Control de bots y AWS WAF Grupo de reglas de control de bots.
- SDK de integración de aplicaciones cliente: valide las sesiones de los clientes y los usuarios finales en sus páginas web y adquiera AWS WAF tokens para que los clientes los utilicen en sus solicitudes web. Si usa ACFP, ATP o control de bots, implemente los SDK de integración de aplicaciones en su aplicación cliente si es posible para aprovechar al máximo todas las características del grupo de reglas. Solo recomendamos utilizar estos grupos de reglas sin una integración de SDK como medida temporal, cuando sea necesario proteger rápidamente un recurso fundamental y no haya tiempo suficiente para la integración de SDK. Para obtener información acerca de cómo implementar los SDK, consulte AWS WAF integración de aplicaciones cliente.
- Challengey acciones de CAPTCHA reglas: valide las sesiones de los clientes y los usuarios finales y adquiera AWS WAF tokens para que los clientes los utilicen en sus solicitudes web.

Puede implementarlos en cualquier lugar en el que especifique una acción de regla, en sus reglas y como sustitutos en los grupos de reglas que utilice. Estas acciones utilizan AWS WAF JavaScript intersticiales para interrogar al cliente o al usuario final, y requieren aplicaciones cliente compatibles. JavaScript Para obtener más información, consulte CAPTCHAy Challenge en AWS WAF.

Los grupos de reglas inteligentes de mitigación de amenazas AWS Managed Rules (ACFP, ATP y Bot Control) utilizan tokens para la detección avanzada. Para obtener información sobre las características que los tokens habilitan en los grupos de reglas, consulte Motivos por los que debería utilizar los SDK de integración de aplicaciones con ACFP, Motivos por los que debería utilizar los SDK de integración de aplicaciones con ATP yMotivos por los que debería utilizar los SDK de integración de aplicaciones con el control de bots.

Sus opciones para implementar una mitigación inteligente de amenazas van desde el uso básico de reglas para gestionar los desafíos y forzar la adquisición de fichas, hasta las funciones avanzadas que ofrecen los grupos de reglas de reglas AWS gestionadas para la mitigación inteligente de amenazas.

En las tablas siguientes se ofrecen comparaciones detalladas de las opciones de las características básicas y avanzadas.

Temas

- Desafíos y adquisición de tokens
- Grupos de reglas administrados para la mitigación de amenazas inteligentes
- Opciones para limitar las tasas en las reglas basadas en tasas y en las reglas específicas de control de bots

Desafíos y adquisición de tokens

Puede proporcionar desafíos y adquirir fichas mediante los SDK de integración de AWS WAF aplicaciones o las acciones de reglas Challenge yCAPTCHA. En términos generales, las acciones de las reglas son más fáciles de implementar, pero incurren en costos adicionales, interfieren más en la experiencia del cliente y son obligatorias. JavaScript Los SDK requieren programación en las aplicaciones cliente, pero pueden proporcionar una mejor experiencia al cliente, son de uso gratuito y se pueden usar con JavaScript o en aplicaciones de Android o iOS. Los SDK de integración de aplicaciones solo se pueden utilizar con las ACL web que utilicen uno de los grupos de reglas

administrados de pago de mitigación de amenazas inteligentes, que se describen en la siguiente sección.

Comparación de opciones para los desafíos y la adquisición de tokens

	Acción de la regla de Challenge	Acción de la regla de CAPTCHA	JavaScript El desafío del SDK	Desafío del SDK para móviles
Definición	Regla una acción que impone la adquisición del AWS WAF token al presentar al cliente del navegador un desafío interstic ial silencioso	Regla una acción que impone la adquisición del AWS WAF token al presentar al cliente (usuario final) un desafío visual o sonoro intersticial	Capa de integración de aplicacio nes, para los navegadores de los clientes y otros dispositivos que se ejecuten. JavaScript Renderiza el desafío silencios o y adquiere un token	Capa de integración de aplicaciones, para aplicacio nes de Android e iOS. Renderiza el desafío silencioso de forma nativa y adquiere un token
Buena elección para...	Validación silenciosa contra las sesiones de bots y aplicación de la adquisición de tokens para los clientes que ofrecen soporte JavaScript	Validación silenciosa y por parte del usuario final contra las sesiones de bots y aplicación de la adquisición de tokens, para los clientes que brindan soporte JavaScript	Validación silenciosa contra las sesiones de bots y aplicación de la adquisición de tokens para los clientes que prestan soporte JavaScript. Los SDK proporcionan la latencia más baja y el mejor control sobre	Validación silenciosa contra las sesiones de bots y aplicación de la adquisición de tokens para aplicaciones móviles nativas en Android e iOS. Los SDK proporcionan la latencia más baja y el mejor

	Acción de la regla de Challenge	Acción de la regla de CAPTCHA	JavaScript El desafío del SDK	Desafío del SDK para móviles
			dónde se ejecuta el script de desafío en la aplicación.	control sobre dónde se ejecuta el script de desafío en la aplicación.
Consideraciones de implement ación	Implementado como configura ción de una acción de regla	Implementado como configura ción de una acción de regla	Requiere uno de los grupos de reglas de pago de ACFP, ATP o control de bots de la ACL web. Requiere codificación en la aplicación cliente.	Requiere uno de los grupos de reglas de pago de ACFP, ATP o control de bots de la ACL web. Requiere codificación en la aplicación cliente.
Consideraciones sobre el tiempo de ejecución	Flujo intrusivo de solicitudes sin tokens válidos. El cliente es redirigido a un AWS WAF desafío interstic ial. Añade viajes de ida y vuelta a la red, y requiere una segunda evaluación de la solicitud web.	Flujo intrusivo de solicitudes sin tokens válidos. El cliente es redirigido a un desafío interstic ial de CAPTCHA AWS WAF . Añade viajes de ida y vuelta a la red, y requiere una segunda evaluación de la solicitud web.	Se puede ejecutar entre bastidores. Le da más control sobre la experiencia del desafío.	Se puede ejecutar entre bastidores. Le da más control sobre la experiencia del desafío.

	Acción de la regla de Challenge	Acción de la regla de CAPTCHA	JavaScript El desafío del SDK	Desafío del SDK para móviles
Requiere JavaScript	Sí	Sí	Sí	No
Clientes compatibles	Navegador y dispositivos que ejecutan Javascript	Navegador y dispositivos que ejecutan Javascript	Navegador y dispositivos que ejecutan Javascript	Dispositivos Android e iOS
Admite aplicaciones de una sola página (SPA)	Solo aplicación. Puede usar la acción Challenge junto con los SDK para asegurarse de que las solicitudes tengan un token de desafío válido. No puede usar la acción de regla para enviar el script del desafío a la página.	Solo aplicación. Puede usar la acción CAPTCHA junto con los SDK para asegurarse de que las solicitudes tengan un token de CAPTCHA válido. No puede usar la acción de regla para enviar el script de CAPTCHA a la página.	Sí	N/A

	Acción de la regla de Challenge	Acción de la regla de CAPTCHA	JavaScript El desafío del SDK	Desafío del SDK para móviles
costos adicionales	Sí, para las configuraciones de acción que especifique explícitamente, ya sea en las reglas que defina o como anulaciones de acciones de regla en los grupos de reglas que utilice. No en todos los demás casos.	Sí, para las configuraciones de acción que especifique explícitamente, ya sea en las reglas que defina o como anulaciones de acciones de regla en los grupos de reglas que utilice. No en todos los demás casos.	No, pero requiere uno de los grupos de reglas de pago de ACFP, ATP o control de bots.	No, pero requiere uno de los grupos de reglas de pago de ACFP, ATP o control de bots.

Para obtener más información sobre los costos asociados a estas opciones, consulte la información sobre la mitigación de amenazas inteligentes en Precios de AWS WAF.

Puede resultar más sencillo plantear desafíos y garantizar una aplicación básica de los símbolos con tan solo agregar una regla con una Challenge o una CAPTCHA acción. Es posible que tenga que usar las acciones de regla, por ejemplo, si no tiene acceso al código de la aplicación.

Sin embargo, si puede implementar los SDK, podrá ahorrar costos y reducir la latencia en la evaluación de la ACL web de las solicitudes web de los clientes, en comparación con la acción Challenge:

- Puede escribir la implementación del SDK para ejecutar el desafío en cualquier punto de la aplicación. Puede adquirir el token en segundo plano, antes de cualquier acción del cliente que pueda enviar una solicitud web a su recurso protegido. De esta forma, el token estará disponible para enviarlo con la primera solicitud de su cliente.
- Si, por el contrario, adquiere los tokens implementando una regla con la acción Challenge, la regla y la acción requieren una evaluación y un procesamiento adicionales de las solicitudes

web cuando el cliente envía una solicitud por primera vez y cada vez que el token caduque. La acción Challenge bloquea la solicitud que no tiene un token válido y vigente, y devuelve el desafío intersticial al cliente. Una vez que el cliente responde correctamente al desafío, el intersticial vuelve a enviar la solicitud web original con el token válido, que luego es evaluado por segunda vez por la ACL web.

Grupos de reglas administrados para la mitigación de amenazas inteligentes

Los grupos de reglas de reglas AWS gestionadas de mitigación inteligente de amenazas proporcionan la gestión de bots básicos, la detección y mitigación de bots sofisticados y maliciosos, la detección y mitigación de los intentos de apropiación de cuentas y la detección y mitigación de los intentos de creación de cuentas fraudulentas. Estos grupos de reglas, combinados con los SDK de integración de aplicaciones descritos en la sección anterior, proporcionan las protecciones más avanzadas y una conexión segura con las aplicaciones cliente.

Comparación de las opciones de grupos de reglas administrados

	ACFP	ATP	Nivel común de control de bots	Nivel objetivo de control de bots
Definición	Gestiona las solicitudes que podrían formar parte de intentos fraudulentos de creación de cuentas en las páginas de registro de una aplicación. No administra los bots. Consulte AWS WAF Grupo de reglas de prevención del	Administra las solicitudes que podrían formar parte de intentos malintencionados de apropiación en la página de inicio de sesión de una aplicación. No administra los bots. Consulte AWS WAF Grupo de reglas de prevención de	Administra bots comunes que se identifican a sí mismos con firmas que son únicas en todas las aplicaciones. Consulte AWS WAF Grupo de reglas de control de bots.	Administra los bots específicos que no se identifican a sí mismos con firmas que son específicas de una aplicación. Consulte AWS WAF Grupo de reglas de control de bots.

	ACFP	ATP	Nivel común de control de bots	Nivel objetivo de control de bots
	fraude (ACFP) para la creación de cuentas de Control de Fraude.	apropiación de cuentas (ATP) para el control del fraude.		

	ACFP	ATP	Nivel común de control de bots	Nivel objetivo de control de bots
Buena elección para...	Inspección del tráfico de creación de cuentas para detectar ataques de creación de cuentas fraudulentas, como los intentos de creación de cuentas con el recorrido del nombre de usuario y la creación de muchas cuentas nuevas a partir de una sola dirección IP.	Inspección del tráfico de inicio de sesión para detectar ataques de apropiación de cuentas, como intentos de inicio de sesión con recorrido de contraseña y muchos intentos de inicio de sesión desde la misma dirección IP. Cuando se usa con tokens, también proporciona protecciones agregadas, como limitar la velocidad de las IP y las sesiones de los clientes en caso de grandes volúmenes de intentos fallidos de inicio de sesión.	Protección básica contra bots y etiquetado del tráfico de bots común y automatizado.	Protección específica contra bots sofisticados, incluida la limitación de las tasas para la sesión del cliente y la detección y mitigación de las herramientas de automatización del navegador, como Selenium y Puppeteer.

	ACFP	ATP	Nivel común de control de bots	Nivel objetivo de control de bots
Añade etiquetas que indican los resultados de la evaluación	Sí	Sí	Sí	Sí
Añade etiquetas de token	Sí	Sí	Sí	Sí
Bloqueo de solicitudes que no tienen un token válido	No incluido. Consulte Bloquear solicitudes que no tienen un AWS WAF token válido.	No incluido. Consulte Bloquear solicitudes que no tienen un AWS WAF token válido.	No incluido. Consulte Bloquear solicitudes que no tienen un AWS WAF token válido.	Bloquea las sesiones de los clientes que envían 5 solicitudes sin un token.
Requiere el token AWS WAF `aws-waf-token`	Obligatorio para todas las reglas. Consulte Motivos por los que debería utilizar los SDK de integración de aplicaciones con ACFP.	Obligatorio para muchas reglas. Consulte Motivos por los que debería utilizar los SDK de integración de aplicaciones con ATP.	No	Sí
Adquiere el AWS WAF token `aws-waf-token`	Sí, lo hace cumplir la regla `AllRequests`	No	No	Algunas reglas utilizan las acciones de regla Challenge o CAPTCHA, que adquieren tokens.

Para obtener más información sobre los costos asociados a estas opciones, consulte la información sobre la mitigación de amenazas inteligentes en Precios de AWS WAF.

Opciones para limitar las tasas en las reglas basadas en tasas y en las reglas específicas de control de bots

Tanto el nivel objetivo del grupo de reglas de control de AWS WAF bots como la declaración de reglas AWS WAF basada en la tasa proporcionan una limitación de la tasa de solicitudes web. En la tabla siguiente se comparan las dos opciones.

Comparación de las opciones de detección y mitigación basadas en tasas

	AWS WAF regla basada en la tasa	AWS WAF Reglas específicas de Bot Control	
Cómo se aplica el límite de tasas	Actúa en función de grupos de solicitud es que llegan a un ritmo demasiado alto. Puede aplicar cualquier acción exceptoAllow:	Aplica patrones de acceso similares a los de las personas y aplica una limitación dinámica de las tasas mediante el uso de tokens de solicitud.	
¿Basado en líneas base históricas de tráfico?	No	Sí	
Tiempo necesario para acumular las líneas base históricas de tráfico	N/A	Cinco minutos para los umbrales dinámicos. N/A para el token ausente.	
Retraso de mitigación	Por lo general, de 30 a 50 segundos. Puede tardar varios minutos.	Normalmente, menos de 10 segundos. Puede tardar varios minutos.	

	AWS WAF regla basada en la tasa	AWS WAF Reglas específicas de Bot Control	
Objetivos de mitigación	Configurable. Puede agrupar las solicitudes mediante una declaración de alcance reducido y mediante una o más claves de agregación, como la dirección IP, el método HTTP y la cadena de consulta.	Direcciones IP y sesiones de cliente	
Nivel de volumen de tráfico necesario para activar las mitigaciones	Medio: pueden ser tan solo 100 solicitudes en el intervalo de tiempo especificado	Bajo: diseñado para detectar patrones de clientes, como rastreadores lentos	
Umbrales personalizables	Sí	No	
Acción de mitigación predeterminada	El valor predeterminado de la consola es Block. No hay una configuración predeterminada en la API; la configuración es obligatoria. Puede configurarlo para cualquier acción de regla exceptoAllow.	La configuración de las acciones de regla del grupo de reglas es Challenge para la ausencia de token y CAPTCHA para el tráfico de gran volumen desde una sola sesión de cliente. Puede configurar cualquiera de estas reglas para cualquier acción de regla válida.	

	AWS WAF regla basada en la tasa	AWS WAF Reglas específicas de Bot Control	
Resiliencia frente a ataques muy distribuidos	Medio: 10 000 direcciones IP como máximo para la limitación de direcciones IP por sí sola	Medio: limitado a un total de 50 000 entre direcciones IP y tokens	
AWS WAF Precios	Incluido en las tarifas estándar de AWS WAF.	Incluido en las tarifas correspondientes al nivel objetivo de mitigación inteligente de amenazas de Bot Control.	
Para obtener más información	Instrucción de regla basada en frecuencia	AWS WAF Grupo de reglas de control de bots	

Las prácticas recomendadas para la mitigación inteligente de amenazas

Siga las prácticas recomendadas de esta sección para lograr la implementación más eficiente y rentable de las características de mitigación de amenazas inteligentes.

- Implemente los SDK de integración de aplicaciones móviles JavaScript y los SDK: implemente la integración de aplicaciones para habilitar el conjunto completo de funciones de ACFP, ATP o Bot Control de la manera más eficaz posible. Los grupos de reglas administrados utilizan los tokens proporcionados por los SDK para separar el tráfico de clientes legítimo del tráfico no deseado a nivel de sesión. Los SDK de integración de aplicaciones garantizan que estos tokens estén siempre disponibles. Para obtener más información, consulte los siguientes temas:
  - Motivos por los que debería utilizar los SDK de integración de aplicaciones con ACFP
  - Motivos por los que debería utilizar los SDK de integración de aplicaciones con ATP
  - Motivos por los que debería utilizar los SDK de integración de aplicaciones con el control de bots

Utilice las integraciones para implementar desafíos en su cliente y, además JavaScript, para personalizar la forma en que se presentan los rompecabezas de CAPTCHA a sus usuarios finales. Para obtener más detalles, consulte AWS WAF integración de aplicaciones cliente.

Si personalizas los rompecabezas de CAPTCHA mediante la JavaScript API y utilizas la acción de la CAPTCHA regla en cualquier parte de tu ACL web, sigue las instrucciones para gestionar la respuesta de AWS WAF CAPTCHA en tu cliente en. Gestión de una respuesta CAPTCHA de AWS WAF Esta guía se aplica a todas las reglas que utilicen esta acción CAPTCHA, incluidas las del grupo de reglas administrado de la ACFP y el nivel de protección específica del grupo de reglas administrado de control de bots.

- Limite las solicitudes que envíe a los grupos de reglas de la ACFP, la ATP y el control de bots. Si utiliza los grupos de reglas gestionadas para la mitigación inteligente de amenazas, tendrá que pagar tasas adicionales. AWS El grupo de reglas de la ACFP inspecciona las solicitudes dirigidas a los puntos conexión de registro y creación de cuentas que especifique. El grupo de reglas de la ATP inspecciona las solicitudes al punto de conexión de inicio de sesión que especifique. El grupo de reglas de control de bots inspecciona todas las solicitudes que llegan a él en la evaluación de la ACL web.

  Tenga en cuenta los siguientes enfoques para reducir el uso de estos grupos de reglas:

  - Excluya las solicitudes de la inspección con una instrucción de restricción de acceso en la instrucción del grupo de reglas administrado. Puede hacerlo con cualquier instrucción anidable. Para obtener más información, consulte Instrucciones de restricción de acceso.
  - Para excluir las solicitudes de la inspección, agregue reglas antes del grupo de reglas. En el caso de las reglas que no puede utilizar en una instrucción de restricción de acceso y en situaciones más complejas, como el etiquetado seguido de una coincidencia de etiquetas, tal vez desee agregar reglas que se ejecuten antes que los grupos de reglas. Para obtener más información, consulte Instrucciones de restricción de acceso y Conceptos básicos de las instrucciones de regla.
  - Ejecute los grupos de reglas tras las reglas menos costosas. Si tienes otras AWS WAF reglas estándar que bloquean las solicitudes por cualquier motivo, ejecútalas antes que estos grupos de reglas de pago. Para obtener más información acerca de las reglas y la administración de reglas, consulte Conceptos básicos de las instrucciones de regla.
  - Si utiliza más de uno de los grupos de reglas administrados de mitigación de amenazas inteligentes, ejecútelos en el siguiente orden para mantener bajos los costos: control de bots, ATP y ACFP.

Para obtener información detallada sobre precios, consulte Precios de AWS WAF.

- Activar el nivel de protección específico del grupo de reglas de control de bots durante el tráfico web normal: algunas reglas del nivel de protección específico necesitan tiempo para establecer líneas base para los patrones de tráfico normales antes de poder reconocer los patrones de tráfico irregulares o maliciosos, y responder a ellos. Por ejemplo, las reglas `TGT_ML_*` necesitan hasta 24 horas para prepararse.

  Añada estas protecciones cuando no esté sufriendo un ataque y deje tiempo para que establezcan sus líneas base antes de esperar que respondan adecuadamente a los ataques. Si agrega estas reglas durante un ataque, después de que el ataque disminuya, el tiempo necesario para establecer una línea base suele oscilar entre el doble y el triple del tiempo normal requerido debido a la asimetría que añade el tráfico de ataques. Para obtener información adicional sobre las reglas y los tiempos de preparación que requieren, consulte Lista de reglas.
- Para la protección contra la denegación de servicio distribuido (DDoS), utilice la mitigación automática de DDoS de la capa de aplicación de Shield Advanced: los grupos de reglas de mitigación de amenazas inteligentes no ofrecen protección contra DDoS. La ACFP lo protege de los intentos fraudulentos de creación de cuentas en la página de registro de su aplicación. La ATP protege su página de inicio de sesión contra los intentos de apropiación de cuentas. El control de bots se centra en aplicar patrones de acceso similares a los humanos mediante tokens y una limitación dinámica de las tasas en las sesiones de los clientes.

  Cuando utiliza Shield Advanced con la mitigación automática de DDoS en la capa de aplicación habilitada, Shield Advanced responde automáticamente a los ataques DDoS detectados creando, evaluando e implementando AWS WAF mitigaciones personalizadas en su nombre. Para obtener más información sobre Shield Advanced, consulte AWS Shield Advanced visión general y AWS Shield Advanced protecciones de capa de aplicación (capa 7).
- Ajustar y configurar la gestión de los tokens: ajuste la gestión de los tokens de la ACL web para obtener la mejor experiencia de usuario.
  - Para reducir los costos operativos y mejorar la experiencia del usuario final, ajuste los tiempos de inmunidad para la gestión de los tokens al máximo que permitan sus requisitos de seguridad. Esto reduce al mínimo el uso de rompecabezas de CAPTCHA y desafíos silenciosos. Para obtener más información, consulte Caducidad de la marca de tiempo: tiempos de inmunidad AWS WAF simbólica.

  - Para permitir el uso compartido de tokens entre aplicaciones protegidas, configure una lista de dominios tokens para su ACL web. Para obtener más información, consulte AWS WAF dominios simbólicos y listas de dominios.
- Rechazar las solicitudes con especificaciones de host arbitrarias: configure sus recursos protegidos para que los encabezados de `Host` de las solicitudes web coincidan con el recurso objetivo. Puede aceptar un valor o un conjunto específico de valores, por ejemplo, `myExampleHost.com` y `www.myExampleHost.com`, pero no acepte valores arbitrarios para el host.
- Para ver los balanceadores de carga de aplicaciones que son orígenes de CloudFront distribuciones, CloudFront configúrelos y AWS WAF administre los tokens de manera adecuada: si asocia su ACL web a un balanceador de carga de aplicaciones e implementa el balanceador de carga de aplicaciones como origen de una distribución, consulte. CloudFront Configuración requerida para los balanceadores de carga de aplicaciones que son orígenes CloudFront
- Probar y ajustar antes de la implementación: antes de implementar cualquier cambio en su ACL web, siga los procedimientos de prueba y ajuste de esta guía para asegurarse de que obtiene el comportamiento esperado. Esto es especialmente importante para estas características de pago. Para obtener orientación general, consulte Probando y ajustando sus AWS WAF protecciones. Para obtener información específica a los grupos de reglas de reglas administradas pagadas, consulte Pruebas implementación de la ACFP, Pruebas e implementación de la ATP y Prueba e implementación de AWS WAF Bot Control.

AWS WAF tokens de solicitud web

AWS WAF los tokens son una parte integral de las protecciones mejoradas que ofrece la mitigación AWS WAF inteligente de amenazas. Un token, a veces denominado huella digital, es una recopilación de información sobre una sesión de un solo cliente que el cliente almacena y proporciona con cada solicitud web que envía. AWS WAF usa tokens para identificar y separar las sesiones de clientes maliciosos de las sesiones legítimas, incluso cuando ambas se originan en una sola dirección IP. El uso de los tokens supone unos costos insignificantes para los usuarios legítimos, pero caros a escala para las botnets.

AWS WAF utiliza tokens para respaldar su navegador y la funcionalidad de impugnación para el usuario final, que proporcionan los SDK de integración de aplicaciones y las acciones de las reglas Challenge yCAPTCHA. Además, los tokens incorporan funciones de los grupos de reglas gestionados para el control de AWS WAF bots y la prevención de apropiación de cuentas.

AWS WAF crea, actualiza y cifra los tokens para los clientes que responden con éxito a los desafíos silenciosos y a los puzles CAPTCHA. Cuando un cliente con un token envía una solicitud web, incluye el token cifrado, lo AWS WAF descifra y verifica su contenido.

Temas

Cómo AWS WAF usa los tokens

AWS WAF usa tokens para registrar y verificar los siguientes tipos de validación de la sesión del cliente:

- CAPTCHA: los rompecabezas de CAPTCHA ayudan a distinguir a los bots de los usuarios humanos. Un CAPTCHA solo se ejecuta mediante la acción de regla CAPTCHA. Al completar con éxito el rompecabezas, el script CAPTCHA actualiza la marca de tiempo del CAPTCHA del token. Para obtener más información, consulte CAPTCHAy Challenge en AWS WAF.
- Desafío: los desafíos se ejecutan de forma silenciosa para ayudar a distinguir las sesiones normales de los clientes de las sesiones de bots y hacer que su funcionamiento sea más costoso para los bots. Cuando el desafío se completa correctamente, el script de desafío obtiene automáticamente un nuevo token AWS WAF si es necesario y, a continuación, actualiza la marca temporal del desafío del token.

  AWS WAF ejecuta desafíos en las siguientes situaciones:

  - SDK de integración de aplicaciones: los SDK de integración de aplicaciones se ejecutan dentro de las sesiones de la aplicación cliente y ayudan a garantizar que los intentos de inicio de sesión solo se permitan después de que el cliente haya respondido correctamente a un desafío. Para obtener más información, consulte AWS WAF integración de aplicaciones cliente.

- regla de acción de Challenge: para obtener más información sobre las acciones de las reglas, consulte CAPTCHAy Challenge en AWS WAF.
- CAPTCHA: cuando se ejecuta un intersticial CAPTCHA, si el cliente aún no tiene un token, el script ejecuta primero automáticamente un desafío para verificar la sesión del cliente e inicializar el token.

Muchas de las reglas de los grupos de reglas de las reglas AWS gestionadas por amenazas inteligentes requieren fichas. Las reglas utilizan tokens para hacer cosas como distinguir entre los clientes a nivel de sesión, determinar las características del navegador y comprender el nivel de interactividad humana en la página web de la aplicación. Estos grupos de reglas invocan la administración de AWS WAF fichas, que aplica un etiquetado de fichas que luego inspeccionan los grupos de reglas.

- AWS WAF Control del fraude y prevención del fraude en la creación de cuentas (ACFP): las normas de la ACFP exigen que las solicitudes web se realicen con tokens válidos. Para obtener más información acerca de las reglas, consulte AWS WAF Grupo de reglas de prevención del fraude (ACFP) para la creación de cuentas de Control de Fraude.
- AWS WAF Control del fraude y prevención de la apropiación de cuentas (ATP): las normas de la ATP que impiden que las sesiones con clientes sean muy voluminosas y duren mucho tiempo, exigen que las solicitudes web estén acompañadas de un token válido y una fecha de impugnación indefinida. Para obtener más información, consulte AWS WAF Grupo de reglas de prevención de apropiación de cuentas (ATP) para el control del fraude.
- AWS WAF Control de bots: las reglas específicas de este grupo de reglas limitan la cantidad de solicitudes web que un cliente puede enviar sin un token válido y utilizan el seguimiento de las sesiones mediante un token para la supervisión y la gestión de las sesiones. Según sea necesario, las reglas aplican las acciones de regla Challenge y CAPTCHA para aplicar la adquisición de los tokens y un comportamiento válido del cliente. Para obtener más información, consulte AWS WAF Grupo de reglas de control de bots.

AWS WAF características del token

Cada token incluye las siguientes características:

- El token se almacena en una cookie llamada `aws-waf-token`.
- El token está cifrado.

- El token toma las huellas digitales de la sesión del cliente con un identificador granular fijo que contiene la siguiente información:
  - La marca de tiempo de la última respuesta exitosa del cliente a un desafío silencioso.
  - La marca de tiempo de la última respuesta exitosa del usuario final a un desafío silencioso. Esto solo está presente si utiliza el CAPTCHA en sus protecciones.
  - Información adicional sobre el cliente y su comportamiento que puede ayudar a separar a sus clientes legítimos del tráfico no deseado. La información incluye varios identificadores de clientes y señales del cliente que se pueden utilizar para detectar actividades automatizadas. La información recopilada no es única y no se puede asignar a un ser humano individual.
    - Todos los tokens incluyen datos de las consultas del navegador del cliente, como indicios de automatización e incoherencias en la configuración del navegador. Los scripts que ejecuta la acción Challenge y los SDK de la aplicación cliente recuperan esta información. Los scripts interrogan activamente al navegador y colocan los resultados en el token.
    - Además, al implementar un SDK de integración de aplicaciones cliente, el token incluye información recopilada de forma pasiva sobre la interactividad del usuario final con la página de la aplicación. La interactividad incluye los movimientos del ratón, las pulsaciones de teclas y las interacciones con cualquier formulario HTML que esté presente en la página. Esta información ayuda a AWS WAF a detectar el nivel de interactividad humana en el cliente, lo que supone un desafío para los usuarios que no parecen humanos. Para obtener información acerca de las integraciones del cliente, consulte AWS WAF integración de aplicaciones cliente.

Por motivos de seguridad, AWS no proporciona una descripción completa del contenido de los AWS WAF tokens ni información detallada sobre el proceso de cifrado de los tokens.

Caducidad de la marca de tiempo: tiempos de inmunidad AWS WAF simbólica

AWS WAF utiliza los tiempos de desafío y de inmunidad al CAPTCHA para controlar la frecuencia con la que se puede presentar un desafío o un CAPTCHA a una sesión de un solo cliente. Una vez que un usuario final responde satisfactoriamente a un CAPTCHA, el tiempo de inmunidad del CAPTCHA determina cuánto tiempo el usuario final permanece inmune a la presentación de otro CAPTCHA. Del mismo modo, el tiempo de inmunidad del desafío determina cuánto tiempo una sesión de cliente permanece inmune a la posibilidad de volver a ser desafiada tras responder satisfactoriamente a un desafío.

AWS WAF registra una respuesta exitosa a un desafío o CAPTCHA actualizando la marca de tiempo correspondiente dentro del token. Al AWS WAF inspeccionar el token en busca de un desafío o un CAPTCHA, resta la marca de tiempo de la hora actual. Si el resultado es superior al tiempo de inmunidad configurado, la marca de tiempo caduca.

Puede configurar los tiempos de inmunidad del CAPTCHA y el desafío en la ACL web y también en cualquier regla que utilice la acción de regla CAPTCHA o Challenge.

- La configuración predeterminada de la ACL web para ambos tiempos de inmunidad es de 300 segundos.
- Puede especificar el tiempo de inmunidad para cualquier regla que utilice la acción CAPTCHA o Challenge. Si no especifica el tiempo de inmunidad de la regla, esta hereda la configuración de la ACL web.
- En el caso de una regla de un grupo de reglas que utilice la acción CAPTCHA o Challenge, si no especifica el tiempo de inmunidad de la regla, esta heredará la configuración de cada ACL web en la que utilice el grupo de reglas.
- Los SDK de integración de aplicaciones utilizan el tiempo de inmunidad de los desafíos de la ACL web.

El valor mínimo del tiempo de inmunidad del desafío es 300 segundos. El valor mínimo del tiempo de inmunidad de CAPTCHA es 60 segundos. El valor máximo para ambos tiempos de inmunidad es de 259 200 segundos o tres días.

Puede utilizar la ACL web y la configuración del tiempo de inmunidad en la regla para ajustar la acción CAPTCHA, Challenge o el comportamiento de administración de desafíos del SDK. Por ejemplo, puede configurar reglas que controlen el acceso a datos muy confidenciales con tiempos de inmunidad bajos y, a continuación, establecer tiempos de inmunidad más altos en la ACL web para que los hereden las demás reglas y los SDK.

En el caso concreto del CAPTCHA, resolver un rompecabezas puede arruinar la experiencia del cliente en el sitio web, por lo que ajustar el tiempo de inmunidad del CAPTCHA puede ayudarle a mitigar el impacto en la experiencia del cliente y, al mismo tiempo, ofrecer las protecciones que desea.

Para obtener información adicional sobre cómo ajustar los tiempos de inmunidad para su uso de las acciones de regla Challenge y CAPTCHA, consulte Prácticas recomendadas para usar las acciones CAPTCHA y Challenge.

Dónde configurar los tiempos de inmunidad AWS WAF simbólicos

Puede establecer los tiempos de inmunidad en su ACL web y en las reglas que utilizan las acciones de regla Challenge y CAPTCHA.

Para obtener información general sobre la administración de una ACL web y sus reglas, consulte Trabajar con ACL web.

Dónde configurar el tiempo de inmunidad de una ACL web

- Consola: al editar la ACL web, en la pestaña Reglas, edite y cambie la configuración de los paneles de Configuración de CAPTCHA de ACL web y Configuración de desafíos de ACL web. En la consola, solamente puede configurar los tiempos de inmunidad de los CAPTCHA y los desafíos de la ACL web después de haber creado la ACL web.
- Fuera de la consola: el tipo de datos de la ACL web tiene parámetros de configuración de CAPTCHA y desafíos, que puede configurar y proporcionar a sus operaciones de creación y actualización en la ACL web.

Dónde configurar el tiempo de inmunidad de una regla

- Consola: al crear o editar una regla y especificar la acción CAPTCHA o Challenge, puede modificar la configuración del tiempo de inmunidad de la regla.
- Fuera de la consola: el tipo de datos de la regla tiene parámetros de configuración de CAPTCHA y desafíos, que puede configurar al definir la regla.

AWS WAF dominios simbólicos y listas de dominios

Cuando AWS WAF crea un token para un cliente, lo configura con un dominio de token. Cuando AWS WAF inspecciona un token en una solicitud web, lo rechaza por no válido si su dominio no coincide con ninguno de los dominios que se consideran válidos para la ACL web.

De forma predeterminada, AWS WAF solo acepta los tokens cuya configuración de dominio coincida exactamente con la del dominio host del recurso asociado a la ACL web. Se trata del valor del encabezado `Host` de la solicitud web. En un navegador, puedes encontrar este dominio en la JavaScript `window.location.hostname` propiedad y en la dirección que el usuario ve en la barra de direcciones.

También puede especificar dominios de tokens aceptables en su configuración de ACL web, tal y como se describe en la siguiente sección. En este caso, AWS WAF acepta tanto las coincidencias

exactas con el encabezado del host como las coincidencias con los dominios de la lista de dominios simbólicos.

Puede especificar los dominios simbólicos AWS WAF para usarlos al configurar el dominio y al evaluar un token en una ACL web. Los dominios que especifique no pueden ser sufijos públicos, como `gov.au`. Para ver los dominios que no puede usar, consulte la lista en lista https://publicsuffix.org/list/public_suffix_list.dat en la lista de sufijos públicos.

AWS WAF Configuración de la lista de dominios del token ACL web

Puede configurar una ACL web para compartir los tokens entre varios recursos protegidos proporcionando una lista de dominios simbólicos con los dominios adicionales que desee AWS WAF aceptar. Con una lista de dominios simbólicos, AWS WAF sigue aceptando el dominio anfitrión del recurso. Además, acepta todos los dominios de la lista de dominios de tokens, incluidos sus subdominios prefijados.

Por ejemplo, una especificación de dominio `example.com` de su lista de dominios de tokens coincide con `example.com` (de `http://example.com/`), `api.example.com`, (de `http://api.example.com/`) y `www.example.com` (de `http://www.example.com/`). No coincide con `example.api.com` (de `http://example.api.com/`) ni con `apiexample.com` (de `http://apiexample.com/`).

Puede configurar la lista de dominios de tokens de su ACL web al crearla o editarla. Para obtener información general sobre la administración de una ACL web, consulte Trabajar con ACL web.

AWS WAF configuración de dominio simbólico

AWS WAF crea tokens a petición de los scripts de desafío, que son ejecutados por los SDK de integración de aplicaciones y las acciones de la Challenge CAPTCHA regla.

El dominio que se AWS WAF establece en un token viene determinado por el tipo de script de desafío que lo solicita y por cualquier configuración de dominio de token adicional que proporciones. AWS WAF establece el dominio del token en la configuración más corta y general que pueda encontrar en la configuración.

- JavaScript SDK: puede configurar el JavaScript SDK con una especificación de dominio simbólico, que puede incluir uno o más dominios. Los dominios que configure deben ser dominios que AWS WAF acepten, en función del dominio host protegido y de la lista de dominios simbólicos de la ACL web.

Cuando AWS WAF emite un token para el cliente, establece el dominio del token en uno que coincida con el dominio host y sea el más corto, entre el dominio host y los dominios de la lista configurada. Por ejemplo, si el dominio anfitrión es `api.example.com` y la lista de dominios token tiene`example.com`, AWS WAF usa `example.com` el token porque coincide con el dominio host y es más corto. Si no proporcionas una lista de dominios simbólicos en la configuración de la JavaScript API, AWS WAF establece el dominio como el dominio host del recurso protegido.

Para obtener más información, consulte Suministro de dominios para su uso en los tokens.

- SDK para móviles: en el código de su aplicación, debe configurar el SDK para móviles con una propiedad de dominio de token. Esta propiedad debe ser un dominio que AWS WAF acepte, basándose en el dominio del host protegido y en la lista de dominios de token en ACL web.

  Cuando AWS WAF emite un token para el cliente, este utiliza esta propiedad como dominio del token. AWS WAF no usa el dominio host en los tokens que emite para el cliente del SDK móvil.

  Para obtener más información, consulte la `WAFConfiguration` `domainName` configuración en La especificación del SDK AWS WAF móvil.
- Challengeacción: si especificas una lista de dominios simbólicos en la ACL web, AWS WAF establece el dominio simbólico en uno que coincida con el dominio anfitrión y que sea el más corto, de entre el dominio host y los dominios de la lista. Por ejemplo, si el dominio anfitrión es `api.example.com` y la lista de dominios token tiene`example.com`, AWS WAF usa `example.com` el token porque coincide con el dominio host y es más corto. Si no proporciona una lista de dominios simbólicos en la ACL web, AWS WAF establece el dominio como el dominio host del recurso protegido.

AWS WAF etiquetado de tokens por parte del bot y grupos de reglas gestionados contra el fraude

En esta sección, se describen las etiquetas que la administración de AWS WAF tokens añade a las solicitudes web. Para obtener información general sobre las etiquetas, consulteAWS WAF etiquetas en las solicitudes web.

Cuando utilizas cualquiera de los grupos de reglas gestionados por AWS WAF bots o por el control de fraudes, los grupos de reglas utilizan la gestión de AWS WAF fichas para inspeccionar las fichas de las solicitudes web y etiquetarlas. Para obtener información sobre los grupos de reglas administrados, consulte AWS WAF Grupo de reglas de prevención del fraude (ACFP) para la

creación de cuentas de Control de Fraude, AWS WAF Grupo de reglas de prevención de apropiación de cuentas (ATP) para el control del fraude y AWS WAF Grupo de reglas de control de bots.

> **Note**
>
> AWS WAF aplica etiquetas de token solo cuando se utiliza uno de estos grupos de reglas gestionados de forma inteligente para la mitigación de amenazas.

La administración de token puede agregar las siguientes etiquetas a las solicitudes web.

Etiqueta de sesión de cliente

La etiqueta `awswaf:managed:token:id:`*`identifier`* contiene un identificador único que la administración de AWS WAF tokens utiliza para identificar la sesión del cliente. El identificador puede cambiar, por ejemplo, si el cliente adquiere un nuevo token después de descartar el que estaba utilizando.

> **Note**
>
> AWS WAF no informa de CloudWatch las estadísticas de Amazon para esta etiqueta.

Etiquetas de estado del token: prefijos del espacio de nombres de etiquetas

Las etiquetas de estado del token informan sobre el estado del token y de la información que contiene del desafío y del CAPTCHA.

Cada etiqueta de estado del token comienza con uno de los siguientes prefijos de espacio de nombres:

- `awswaf:managed:token:`: Se utiliza para informar sobre el estado general del token y el estado de la información del desafío del token.
- `awswaf:managed:captcha:`: Se utiliza para informar sobre el estado de la información del CAPTCHA del token.

Etiquetas de estado del token: nombres de etiquetas

Tras el prefijo, el resto de la etiqueta proporciona información detallada sobre el estado del token:

- `accepted`: El token de solicitud está presente y contiene lo siguiente:
  - Una solución válida del desafío o del CAPTCHA.
  - Una marca de tiempo vigente del desafío o del CAPTCHA.
  - Una especificación de dominio válida para la ACL web.

  Ejemplo: la etiqueta `awswaf:managed:token:accepted` indica que el token de la solicitud web tiene una solución válida y una marca temporal vigente para el desafío, así como un dominio válido.
- `rejected`: El token de solicitud está presente, pero no cumple con los criterios de aceptación.

  Junto con la etiqueta rechazada, la administración del token agrega un espacio de nombres y nombre de etiqueta personalizados para indicar el motivo.
  - `rejected:not_solved`: Al token le falta la solución del desafío o del CAPTCHA.
  - `rejected:expired`: La marca temporal del desafío o del CAPTCHA del token ha caducado, de acuerdo con los tiempos de inmunidad del token configurado en la ACL web.
  - `rejected:domain_mismatch`: El dominio del token no coincide con la configuración del dominio del token de su ACL web.
  - `rejected:invalid`— no se AWS WAF pudo leer el token indicado.

  Ejemplo: las etiquetas `awswaf:managed:captcha:rejected` y `awswaf:managed:captcha:rejected:expired` indican que la solicitud se rechazó porque la marca de tiempo del CAPTCHA del token ha superado el tiempo de inmunidad configurado en la ACL web.
- `absent`: La solicitud no contiene el token o el administrador del token no ha podido leerlo.

  Ejemplo: la etiqueta `awswaf:managed:captcha:absent` indica que la solicitud no tiene el token.

Bloquear solicitudes que no tienen un AWS WAF token válido

Cuando utilizas los grupos de reglas AWS gestionadas por amenazas inteligentes `AWSManagedRulesACFPRuleSet` `AWSManagedRulesATPRuleSetAWSManagedRulesBotControlRuleSet`, y los grupos de reglas invocan la administración de AWS WAF tokens para evaluar el estado del token de solicitud web y etiquetar las solicitudes en consecuencia.

> **Note**
>
> El etiquetado de los tokens solo se aplica a las solicitudes web que se evalúan mediante uno de estos grupos de reglas administrados.

Para obtener información sobre el etiquetado que aplica la administración de los tókenes, consulte la sección anterior, AWS WAF etiquetado de tokens por parte del bot y grupos de reglas gestionados contra el fraude.

Luego, los grupos de reglas administrados de mitigación de amenazas inteligentes gestionan los requisitos de los tokens de la siguiente manera:

- La regla `AllRequests` de `AWSManagedRulesACFPRuleSet` está configurada para ejecutar la acción Challenge contra todas las solicitudes y bloquear de forma efectiva las que no tengan la etiqueta de token `accepted`.
- `AWSManagedRulesATPRuleSet` bloquea las solicitudes que tienen la etiqueta de token `rejected`, pero no bloquea las solicitudes con la etiqueta de token `absent`.
- El nivel de protección específica de `AWSManagedRulesBotControlRuleSet` desafía a los clientes después de enviar cinco solicitudes sin una etiqueta de token `accepted`. No bloquea una solicitud individual que no tenga un token válido. El nivel de protección común del grupo de reglas no administra los requisitos de los tokens.

Para obtener más información sobre los grupos de reglas de amenazas inteligentes, consulte AWS WAF Grupo de reglas de prevención del fraude (ACFP) para la creación de cuentas de Control de Fraude, AWS WAF Grupo de reglas de prevención de apropiación de cuentas (ATP) para el control del fraude y AWS WAF Grupo de reglas de control de bots.

Para bloquear las solicitudes a las que les faltan tokens cuando se utiliza el grupo de reglas administrado de control de bots o ATP

Con los grupos de reglas de control de bots y ATP, es posible que una solicitud sin un token válido salga de la evaluación del grupo de reglas y siga siendo evaluada por la ACL web.

Para bloquear todas las solicitudes a las que les falte su token o cuyo token haya sido rechazado, agregue una regla que se ejecute inmediatamente después del grupo de reglas administrado para capturar y bloquear las solicitudes que el grupo de reglas no gestione por usted.

A continuación, se muestra un ejemplo de lista de JSON de una ACL web que utiliza el grupo de reglas administrado de la ATP. La ACL web tiene una regla adicional para capturar la etiqueta `awswaf:managed:token:absent` y gestionarla. La regla limita su evaluación a las solicitudes web que se dirigen al punto de conexión de inicio de sesión para que coincidan con el alcance del grupo de reglas de la ATP. La regla agregada aparece en negrita.

```
{
  "Name": "exampleWebACL",
  "Id": "55555555-6666-7777-8888-999999999999",
  "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/webacl/
exampleWebACL/55555555-4444-3333-2222-111111111111",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesATPRuleSet",
      "Priority": 1,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesATPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesATPRuleSet": {
                "LoginPath": "/web/login",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  }
                },
                "ResponseInspection": {
                  "StatusCode": {
                    "SuccessCodes": [
                      200
                    ],
                    "FailureCodes": [
                      401,
```

```
                    403,
                    500
                  ]
                }
              }
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesATPRuleSet"
    }
  },
  {
    "Name": "RequireTokenForLogins",
    "Priority": 2,
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:token:absent"
              }
            }
          },
          {
            "ByteMatchStatement": {
              "SearchString": "/web/login",
              "FieldToMatch": {
                "UriPath": {}
              },
              "TextTransformations": [
                {
                  "Priority": 0,
                  "Type": "NONE"
                }
```

```
                ],
                "PositionalConstraint": "STARTS_WITH"
              }
            },
            {
              "ByteMatchStatement": {
                "SearchString": "POST",
                "FieldToMatch": {
                  "Method": {}
                },
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ],
                "PositionalConstraint": "EXACTLY"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "RequireTokenForLogins"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "exampleWebACL"
  },
  "Capacity": 51,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111111111111:webacl:exampleWebACL:"
}
```

Configuración requerida para los balanceadores de carga de aplicaciones que son orígenes CloudFront

Lea esta sección si asocia su ACL web a un Application Load Balancer e implementa el Application Load Balancer como origen de una distribución. CloudFront

Con esta arquitectura, debe proporcionar la siguiente configuración adicional para que la información del token se gestione correctamente.

- Configure CloudFront para reenviar la `aws-waf-token` cookie a Application Load Balancer. De forma predeterminada, CloudFront elimina las cookies de la solicitud web antes de reenviarla al origen. Para conservar la cookie de token con la solicitud web, configura el comportamiento de la CloudFront caché para que incluya solo la cookie de token o todas las cookies. Para obtener información sobre cómo hacerlo, consulte Almacenamiento en caché de contenido basado en cookies en la Guía para CloudFront desarrolladores de Amazon.
- AWS WAF Configúrelo para que reconozca el dominio de la CloudFront distribución como un dominio simbólico válido. De forma predeterminada, CloudFront establece el `Host` encabezado en el origen de Application Load Balancer y lo AWS WAF usa como dominio del recurso protegido. Sin embargo, el navegador del cliente ve la CloudFront distribución como el dominio host y los tokens que se generan para el cliente utilizan el CloudFront dominio como dominio del token. Sin ninguna configuración adicional, AWS WAF si se compara el dominio de recursos protegido con el dominio simbólico, se produce una discrepancia. Para solucionar este problema, añada el nombre del dominio de CloudFront distribución a la lista de dominios simbólicos de su configuración de ACL web. Para obtener información acerca de cómo hacerlo, consulte AWS WAF Configuración de la lista de dominios del token ACL web.

AWS WAF Control de fraude: creación de cuentas y prevención del fraude (ACFP)

El fraude en la creación de cuentas es una actividad ilegal en línea en la que un atacante intenta crear una o más cuentas falsas. Los atacantes utilizan cuentas falsas para realizar actividades fraudulentas, como abusar de las bonificaciones promocionales y de registro, hacerse pasar por alguien y los ciberataques, como la suplantación de identidad. La presencia de cuentas falsas puede afectar negativamente a su empresa, ya que perjudica su reputación ante los clientes y la expone al fraude financiero.

Puede supervisar y controlar los intentos de fraude en la creación de cuentas mediante la implementación de la función Control de AWS WAF Fraude y Prevención del Fraude en la Creación de Cuentas (ACFP). AWS WAF ofrece esta función en el grupo de reglas de reglas AWS administradas `AWSManagedRulesACFPRuleSet` con los SDK complementarios de integración de aplicaciones.

El grupo de reglas administrado de la ACFP etiqueta y gestiona las solicitudes que podrían formar parte de intentos malintencionados de creación de cuentas. El grupo de reglas lo hace mediante la inspección de los intentos de creación de cuenta que los clientes envían al punto de conexión de inicio de sesión de la aplicación.

La ACFP protege las páginas de registro de sus cuentas monitorizando las solicitudes de registro de cuentas para detectar actividad anómala y bloqueando automáticamente las solicitudes sospechosas. El grupo de reglas utiliza identificadores de solicitudes, análisis de comportamiento y machine learning para detectar solicitudes fraudulentas.

- Inspección de solicitudes: la ACFP le brinda visibilidad y control sobre los intentos anómalos de creación de cuentas y los intentos en los que se utilizan credenciales robadas con el fin de evitar la creación de cuentas fraudulentas. ACFP comprueba las combinaciones de correo electrónico y contraseña con su base de datos de credenciales robadas, que se actualiza periódicamente a medida que se descubren nuevas credenciales filtradas en la web oscura. La ACFP evalúa los dominios utilizados en las direcciones de correo electrónico y monitoriza el uso de los números de teléfono y los campos de direcciones para verificar las entradas y detectar comportamientos fraudulentos. ACFP agrega los datos por dirección IP y sesión de cliente para detectar y bloquear a los clientes que envían demasiadas solicitudes de naturaleza sospechosa.
- Inspección de respuestas: en el caso de CloudFront las distribuciones, además de inspeccionar las solicitudes de creación de cuentas entrantes, el grupo de reglas de la ACFP inspecciona las respuestas de la aplicación a los intentos de creación de cuentas a fin de hacer un seguimiento de las tasas de éxito y fracaso. Con esta información, ACFP puede bloquear temporalmente las sesiones de los clientes o las direcciones IP que tengan demasiados intentos fallidos. AWS WAF realiza una inspección de las respuestas de forma asíncrona, por lo que no aumenta la latencia del tráfico web.

> **Note**
>
> Se le cobrarán tarifas adicionales cuando utilice este grupo de reglas administrado. Para obtener más información, consulte AWS WAF Precios.

> **Note**
>
> La característica ACFP no está disponible para los grupos de usuarios de Amazon Cognito.

Temas

Componentes de la ACFP

Los componentes principales de la prevención del AWS WAF fraude en la creación de cuentas (ACFP) de Fraud Control son los siguientes:

- **`AWSManagedRulesACFPRuleSet`**— Las reglas de este grupo de reglas AWS administradas detectan, etiquetan y gestionan varios tipos de actividad fraudulenta de creación de cuentas. El grupo de reglas inspecciona las solicitudes de texto/html `GET` HTTP que los clientes envían al punto de conexión de registro de cuentas especificado y las solicitudes web `POST` que los clientes envían al punto de conexión de registro de cuentas especificado. En el caso de CloudFront las distribuciones protegidas, el grupo de reglas también inspecciona las respuestas que la distribución envía a las solicitudes de creación de cuentas. Para obtener una lista de las reglas de este grupo de reglas, consulte AWS WAF Grupo de reglas de prevención del fraude (ACFP) para la creación de cuentas de Control de Fraude. Para incluir este grupo de reglas en su ACL web, utilice una instrucción de referencia de un grupo de reglas administrado. Para obtener información acerca del uso de este grupo de reglas, consulte Adición del grupo de reglas administradas por ACFP a la nueva ACL web.

  > **Note**
  >
  > Se le cobrarán tarifas adicionales cuando utilice este grupo de reglas administrado. Para obtener más información, consulte AWS WAF Precios.

- Detalles sobre las páginas de registro y creación de cuentas de su aplicación: debe proporcionar información sobre las páginas de registro y creación de cuentas al agregar el grupo de reglas `AWSManagedRulesACFPRuleSet` a su ACL web. Esto permite que el grupo de reglas reduzca el alcance de las solicitudes que inspecciona y valide adecuadamente las solicitudes web de creación de cuentas. La página de registro debe aceptar solicitudes de texto/html `GET`. La página de creación de rutas debe aceptar las solicitudes `POST`. El grupo de reglas de la ACFP funciona con nombres de usuario en formato de correo electrónico. Para obtener más información, consulte Adición del grupo de reglas administradas por ACFP a la nueva ACL web.
- En el caso de CloudFront las distribuciones protegidas, detalles sobre cómo responde su aplicación a los intentos de creación de cuentas: usted proporciona detalles sobre las respuestas de la aplicación a los intentos de creación de cuentas y el grupo de reglas de la ACFP rastrea y gestiona los intentos de creación masiva de cuentas desde una única dirección IP o sesión de un solo cliente. Para obtener más información acerca de cómo configurar esta opción, consulte Adición del grupo de reglas administradas por ACFP a la nueva ACL web.
- JavaScript y los SDK de integración de aplicaciones móviles: Implemente los SDK AWS WAF JavaScript y los SDK móviles con su implementación de ACFP para habilitar todo el conjunto de funciones que ofrece el grupo de reglas. Muchas de las reglas de la ACFP utilizan la información proporcionada por los SDK para la verificación de los clientes y la agregación del comportamiento en la sesión, necesarias para separar el tráfico de clientes legítimo del tráfico de bots. Para obtener más información sobre SDKs, consulte AWS WAF integración de aplicaciones cliente.

Puede combinar su implementación de ACFP con lo siguiente para monitorizar, ajustar y personalizar sus protecciones.

- Registro y métricas: puede supervisar su tráfico y comprender cómo lo afecta el grupo de reglas gestionado por la ACFP configurando y habilitando los registros, la recopilación de datos de Amazon Security Lake y CloudWatch las métricas de Amazon para su ACL web. Las etiquetas que se `AWSManagedRulesACFPRuleSet` añaden a sus solicitudes web se incluyen en los datos. Para obtener información sobre las opciones Registro del tráfico de ACL AWS WAF webMonitorización con Amazon CloudWatch, consulte y ¿Qué es Amazon Security Lake? .

  En función de sus necesidades y del tráfico que detecte, es posible que desee personalizar la implementación de `AWSManagedRulesACFPRuleSet`. Por ejemplo, tal vez desee excluir parte del tráfico de la evaluación de la ACFP o modificar la forma en que gestiona algunos de los intentos de fraude en la creación de cuentas que identifica, utilizando AWS WAF funciones como las declaraciones de alcance reducido o las reglas de coincidencia de etiquetas.

- Etiquetas y reglas de coincidencia de etiquetas: para cualquiera de las reglas incluidas en `AWSManagedRulesACFPRuleSet`, puede cambiar el comportamiento de bloqueo a recuento y, a continuación, compararlas con las etiquetas añadidas por las reglas. Utilice este enfoque para personalizar la forma en que gestiona las solicitudes web identificadas por el grupo de reglas administrado de la ACFP. Para obtener más información sobre el etiquetado y el uso de las instrucciones de coincidencia de etiquetas, consulte Instrucción de regla de coincidencia de etiquetas y AWS WAF etiquetas en las solicitudes web.
- Solicitudes y respuestas personalizadas: puede agregar encabezados personalizados a las solicitudes que permita y puede enviar respuestas personalizadas a las solicitudes que bloquee. Para ello, asocie su etiqueta coincidente con las características de solicitud y respuesta personalizadas de AWS WAF . Para obtener más información sobre cómo personalizar las solicitudes y las respuestas, consulte Solicitudes web y respuestas personalizadas en AWS WAF.

Motivos por los que debería utilizar los SDK de integración de aplicaciones con ACFP

Recomendamos encarecidamente implementar los SDK de integración de aplicaciones para un uso más eficiente del grupo de reglas de la ACFP.

- Funcionalidad completa de grupos de reglas: la regla de la ACFP `SignalClientHumanInteractivityAbsentLow` solo funciona con los tokens que se rellenan con las integraciones de aplicaciones. Esta regla detecta y gestiona la interactividad humana anómala con la página de la aplicación. Los SDK de integración de aplicaciones pueden detectar la interactividad humana normal mediante los movimientos del ratón, las pulsaciones de teclas y otras mediciones. Los intersticiales que envían las acciones de regla CAPTCHA y Challenge no pueden proporcionar este tipo de datos.
- Latencia reducida: la regla `AllRequests` del grupo de reglas aplica la acción de regla Challenge a cualquier solicitud que aún no tenga un token de desafío. Cuando esto sucede, el grupo de reglas evalúa la solicitud dos veces: una sin el token y, a continuación, una segunda vez después de haber adquirido el token mediante la acción intersticial Challenge. No se le cobrará ninguna tarifa adicional por usar únicamente la regla `AllRequests`, pero este enfoque agrega una sobrecarga al tráfico web y agrega latencia a la experiencia del usuario final. Si adquiere el token desde el lado del cliente mediante las integraciones de aplicaciones, antes de enviar la solicitud de creación de la cuenta, el grupo de reglas de la ACFP evalúa la solicitud una vez.

Para obtener más información acerca de las capacidades de este grupo de reglas, consulte AWS WAF Grupo de reglas de prevención del fraude (ACFP) para la creación de cuentas de Control de Fraude.

Para obtener información sobre los SDK, consulte AWS WAF integración de aplicaciones cliente. Para obtener información sobre AWS WAF los tokens, consulteAWS WAF tokens de solicitud web. Para obtener información sobre las acciones de las reglas, consulte CAPTCHAy Challenge en AWS WAF.

Adición del grupo de reglas administradas por ACFP a la nueva ACL web

Con el fin de configurar el grupo de reglas administrado de la ACFP para que reconozca las actividades fraudulentas de creación de cuentas en su tráfico web, debe proporcionar información sobre cómo los clientes acceden a su página de registro y enviar las solicitudes de creación de cuentas a su aplicación. En el caso de CloudFront las distribuciones protegidas de Amazon, también debes proporcionar información sobre cómo responde tu aplicación a las solicitudes de creación de cuentas. Esta configuración se suma a la configuración normal de un grupo de reglas administrado.

Para ver la descripción del grupo de reglas y la lista de reglas, consulte AWS WAF Grupo de reglas de prevención del fraude (ACFP) para la creación de cuentas de Control de Fraude.

> **Note**
>
> La base de datos de credenciales robadas de la ACFP solo contiene nombres de usuario en formato de correo electrónico.

Esta guía está destinada a los usuarios que, en general, saben cómo crear y administrar las ACL web, las reglas y los grupos de reglas de AWS WAF . Estos temas se tratan en secciones anteriores de esta guía. Para obtener información básica sobre cómo agregar un grupo de reglas administrado a su ACL web, consulte Adición de un grupo de reglas administrado a una ACL web a través de la consola.

Seguir las prácticas recomendadas

Utilice el grupo de reglas de la ACFP de acuerdo con las prácticas recomendadas de Las prácticas recomendadas para la mitigación inteligente de amenazas.

Uso del grupo de reglas de **`AWSManagedRulesACFPRuleSet`** en su ACL web

1. Añada el grupo de reglas AWS gestionado `AWSManagedRulesACFPRuleSet` a su ACL web y edite la configuración del grupo de reglas antes de guardarlo.

   > **Note**
   >
   > Se le cobrarán tarifas adicionales cuando utilice este grupo de reglas administrado. Para obtener más información, consulte AWS WAF Precios.

2. En el panel configuración del grupo de reglas, proporcione la información que el grupo de reglas de la ACFP utiliza para inspeccionar las solicitudes de creación de cuentas.

   a. En Usar expresiones regulares en las rutas, active esta opción si desea AWS WAF hacer coincidir las expresiones regulares con las especificaciones de las rutas de las páginas de registro y creación de cuentas.

      AWS WAF admite la sintaxis de patrones utilizada por la biblioteca PCRE `libpcre` con algunas excepciones. La biblioteca está documentada en PCRE, expresiones regulares compatibles con Perl. Para obtener información sobre el AWS WAF soporte, consulteCoincidencia de patrones de expresiones regulares en AWS WAF.

   b. En Ruta de la página de registro, indique la ruta del punto de conexión de la página de registro de su aplicación. Esta página debe aceptar solicitudes de texto/html `GET`. El grupo de reglas inspecciona solo las solicitudes de texto/html `GET` HTTP enviadas al punto de conexión de la página de registro especificada.

      > **Note**
      >
      > La coincidencia de puntos de conexión no distingue entre mayúsculas y minúsculas. Las especificaciones de expresiones regulares no deben incluir la marca `(?-i)`, ya que desactiva la coincidencia sin distinción entre mayúsculas y minúsculas. Las especificaciones de las cadenas deben empezar con una barra diagonal `/`.

      Por ejemplo, para la URL `https://example.com/web/registration`, puede proporcionar la especificación de la ruta de la cadena `/web/registration`. Las rutas de las páginas de registro que comienzan con la ruta que proporcione se consideran coincidentes. Por ejemplo, `/web/registration` coincide con las rutas de registro `/`

`web/registration`, `/web/registration/`, `/web/registrationPage` y `/web/registration/thisPage`, pero no coincide con la ruta `/home/web/registration` o `/website/registration`.

> **Note**
>
> Asegúrese de que los usuarios finales carguen la página de registro antes de enviar una solicitud de creación de cuenta. Esto ayuda a garantizar que las solicitudes de creación de cuenta que envía el cliente incluyan tókenes válidos.

c. Para la ruta de creación de la cuenta, proporcione el URI de su sitio web que acepte los detalles completados del nuevo usuario. Este URI debe aceptar solicitudes `POST`.

> **Note**
>
> La coincidencia de puntos de conexión no distingue entre mayúsculas y minúsculas. Las especificaciones de expresiones regulares no deben incluir la marca `(?-i)`, ya que desactiva la coincidencia sin distinción entre mayúsculas y minúsculas. Las especificaciones de las cadenas deben empezar con una barra diagonal `/`.

Por ejemplo, para la URL `https://example.com/web/newaccount`, puede proporcionar la especificación de la ruta de la cadena `/web/newaccount`. Las rutas de creación de cuentas que comienzan con la ruta que usted proporciona se consideran coincidentes. Por ejemplo, `/web/newaccount` coincide con las rutas de creación de cuentas `/web/newaccount`, `/web/newaccount/`, `/web/newaccountPage` y `/web/newaccount/thisPage`, pero no coincide con la ruta `/home/web/newaccount` o `/website/newaccount`.

d. Para Inspeccionar solicitudes, especifique cómo acepta su aplicación los intentos de creación de cuentas. Para ello, proporcione el tipo de carga útil de la solicitud y los nombres de los campos del cuerpo de la solicitud en los que se incluyen el nombre de usuario, la contraseña y otros detalles de creación de la cuenta.

> **Note**
>
> Para los campos de dirección y número de teléfono principales, proporcione los campos en el orden en que aparecen en la carga útil de la solicitud.

La especificación de los nombres de los campos depende del tipo de carga útil.

- Tipo de carga útil JSON: especifique los nombres de los campos en la sintaxis del puntero JSON. Para obtener información sobre la sintaxis del puntero JSON, consulte la documentación del Grupo de trabajo de ingeniería de Internet (IETF) sobre el puntero de notación de JavaScript objetos (JSON).

  Por ejemplo, para el siguiente ejemplo de carga útil JSON, la especificación del campo de nombre de usuario es `/signupform/username` y las especificaciones del campo de dirección principal son `/signupform/addrp1`, `/signupform/addrp2` y `/signupform/addrp3`.

```
{
    "signupform": {
        "username": "THE_USERNAME",
        "password": "THE_PASSWORD",
        "addrp1": "PRIMARY_ADDRESS_LINE_1",
        "addrp2": "PRIMARY_ADDRESS_LINE_2",
        "addrp3": "PRIMARY_ADDRESS_LINE_3",
        "phonepcode": "PRIMARY_PHONE_CODE",
        "phonepnumber": "PRIMARY_PHONE_NUMBER"
    }
}
```

- Tipo de carga útil FORM_ENCODED: use los nombres de los formularios HTML.

  Por ejemplo, para un formulario HTML con elementos de entrada de usuario y contraseña denominados `username1` y `password1`, la especificación del campo de nombre de usuario es `username1` y la especificación del campo de contraseña es `password1`.

e. Si estás protegiendo CloudFront las distribuciones de Amazon, en la inspección de respuestas, especifica cómo indica tu aplicación el éxito o el fracaso en sus respuestas a los intentos de creación de cuentas.

> **Note**
>
> La inspección de respuestas de la ACFP solo está disponible en las ACL web que protegen las distribuciones. CloudFront

Especifique un único componente en la respuesta de creación de la cuenta que desee que inspeccione la ACFP. Para los tipos de componentes Body y JSON, AWS WAF puede inspeccionar los primeros 65.536 bytes (64 KB) del componente.

Indique sus criterios de inspección para el tipo de componente, tal y como se indica en la interfaz. Debe proporcionar los criterios de éxito y fracaso para inspeccionar el componente.

Por ejemplo, supongamos que su solicitud indica el estado de un intento de creación de cuenta en el código de estado de la respuesta y utiliza `200 OK` para indicar si se ha realizado correctamente, y `401 Unauthorized` o `403 Forbidden` si ha fallado. Debe establecer el Tipo de componente de inspección de respuesta en el Código de estado y, a continuación, en el cuadro de texto Éxito, introducir `200`, y, en el cuadro de texto Error, introducir `401` en la primera línea y `403` en la segunda.

El grupo de reglas de la ACFP solo cuenta las respuestas que coinciden con sus criterios de inspección de éxito o fracaso. Las reglas del grupo de reglas actúan sobre los clientes cuando tienen una tasa de éxito demasiado alta entre las respuestas que se cuentan, con el fin de mitigar los intentos de creación masiva de cuentas. Para cumplir con precisión las reglas del grupo de reglas, asegúrese de proporcionar información completa tanto para los intentos de creación de cuentas exitosos como para los fallidos.

Para ver las reglas que inspeccionan las respuestas de creación de cuentas, busque `VolumetricIPSuccessfulResponse` y `VolumetricSessionSuccessfulResponse` en la lista de reglas que aparece en AWS WAF Grupo de reglas de prevención del fraude (ACFP) para la creación de cuentas de Control de Fraude.

3. Proporcione cualquier configuración adicional que desee para el grupo de reglas.

   Puede limitar aún más el alcance de las solicitudes que el grupo de reglas inspecciona agregando una instrucción de restricción de acceso a la instrucción del grupo de reglas administrado. Por ejemplo, solamente puede inspeccionar las solicitudes con un argumento de consulta o una cookie específicos. El grupo de reglas solo inspeccionará las solicitudes que coincidan con los criterios de su instrucción de restricción de acceso y que se envíen a las rutas de registro y creación de cuentas que especificó en la configuración del grupo de reglas. Para obtener información sobre las instrucciones de restricción de acceso, consulte Instrucciones de restricción de acceso.

4. Guarde los cambios en la ACL web.

Antes de implementar cambios en su ACFP para el tráfico de producción, pruébelos y ajústelos en un entorno provisional o de prueba hasta que se sienta cómodo con el posible impacto en el tráfico. A continuación, pruebe y ajuste las reglas en el modo de recuento con el tráfico de producción antes de habilitarlas. Consulte la sección siguiente para obtener orientación.

Pruebas implementación de la ACFP

Esta sección proporciona una guía general para configurar y probar una implementación de la prevención del AWS WAF fraude en la creación de cuentas (ACFP) de Fraud Control para su sitio. Los pasos específicos que elija seguir dependerán de sus necesidades, recursos y solicitudes web que reciba.

Esta información se suma a la información general sobre las pruebas y los ajustes que se proporcionan en Probando y ajustando sus AWS WAF protecciones.

> **Note**
>
> AWS Las reglas administradas están diseñadas para protegerlo de las amenazas web más comunes. Cuando se utilizan de acuerdo con la documentación, los grupos de reglas de reglas AWS administradas añaden otro nivel de seguridad a sus aplicaciones. Sin embargo, los grupos de reglas de reglas AWS administradas no pretenden sustituir sus responsabilidades de seguridad, que vienen determinadas por los AWS recursos que seleccione. Consulte el modelo de responsabilidad compartida para asegurarse de que sus recursos AWS estén debidamente protegidos.

> **Riesgo de tráfico de producción**
>
> Antes de implementar cambios en su ACFP para el tráfico de producción, pruébelos y ajústelos en un entorno provisional o de prueba hasta que se sienta cómodo con el posible impacto en el tráfico. A continuación, pruebe y ajuste las reglas en el modo de recuento con el tráfico de producción antes de habilitarlas.

AWS WAF proporciona credenciales de prueba que puede utilizar para verificar la configuración de la ACFP. En el siguiente procedimiento, configurará una ACL web de prueba para usar el grupo de reglas administrado de la ACFP, configurará una regla para capturar la etiqueta agregada por el grupo de reglas y, a continuación, realizará un intento de creación de cuentas con estas credenciales

de prueba. Verificarás que tu ACL web ha gestionado correctamente el intento comprobando CloudWatch las métricas de Amazon para el intento de creación de la cuenta.

Esta guía está destinada a los usuarios que, en general, saben cómo crear y administrar las ACL web, las reglas y los grupos de reglas de AWS WAF . Estos temas se tratan en secciones anteriores de esta guía.

Para configurar y probar una implementación de AWS WAF Fraud Control, creación de cuentas y prevención del fraude (ACFP)

Realice estos pasos primero en un entorno de prueba y, después, en producción.

1. Agregue el AWS WAF grupo de reglas gestionadas por el Control de Fraude Control de Creación de Cuentas y Prevención del Fraude (ACFP) en el modo de recuento

   > **Note**
   >
   > Se le cobrarán tarifas adicionales cuando utilice este grupo de reglas administrado. Para obtener más información, consulte AWS WAF Precios.

   Agregue el grupo de reglas AWS administradas `AWSManagedRulesACFPRuleSet` a una ACL web nueva o existente y configúrelo para que no altere el comportamiento actual de la ACL web. Para obtener más información sobre las reglas y etiquetas de este grupo de reglas, consulte AWS WAF Grupo de reglas de prevención del fraude (ACFP) para la creación de cuentas de Control de Fraude.

   - Cuando añada el grupo de reglas administrado, edítelo y haga lo siguiente:
     - En el panel de Configuración del grupo de reglas, proporcione los detalles de las páginas de registro y creación de cuentas de su aplicación. El grupo de reglas de la ACFP utiliza esta información para monitorizar las actividades de inicio de sesión. Para obtener más información, consulte Adición del grupo de reglas administradas por ACFP a la nueva ACL web.
     - En el panel Reglas, abra el menú desplegable Anular todas las acciones de reglas y elija Count. Con esta configuración, AWS WAF evalúa las solicitudes comparándolas con todas las reglas del grupo de reglas y solo cuenta las coincidencias resultantes, sin dejar de agregar etiquetas a las solicitudes. Para obtener más información, consulte Invalidar acciones de reglas en un grupo de reglas.

Con esta anulación, puede supervisar el posible impacto de las reglas administradas de ACFP para determinar si desea agregar excepciones, por ejemplo, excepciones para casos de uso interno.

- Sitúe el grupo de reglas de forma que se evalúe según las reglas existentes en la ACL web, con una configuración de prioridad numéricamente superior a la de cualquier regla o grupo de reglas que ya esté utilizando. Para obtener más información, consulte Procesamiento del orden de las reglas y los grupos de reglas en una ACL web.

  De esta forma, no se interrumpe su gestión actual del tráfico. Por ejemplo, si tiene reglas que detectan tráfico malicioso, como la inyección de código SQL o el scripting entre sitios, seguirán detectándolo y registrándolo. Como alternativa, si tiene reglas que permiten el tráfico no malicioso conocido, estas pueden seguir permitiéndolo sin que el grupo de reglas administrado de la ACFP lo bloquee. Puede decidir ajustar el procesamiento de pedidos durante sus actividades de prueba y ajuste.

2. Implementación de los SDK de integración de aplicaciones

   Integre el AWS WAF JavaScript SDK en las rutas de registro y creación de cuentas de su navegador. AWS WAF también proporciona SDK móviles para integrar dispositivos iOS y Android. Para obtener más información acerca de la integración de los SDK, consulte AWS WAF integración de aplicaciones cliente. Para obtener más información sobre esta recomendación, consulte Motivos por los que debería utilizar los SDK de integración de aplicaciones con ACFP.

   > **Note**
   >
   > Si no puede utilizar los SDK de integración de aplicaciones, puede probar el grupo de reglas de la ACFP editándolo en su ACL web y eliminando la anulación que haya colocado en la regla `AllRequests`. Esto habilita la configuración de la acción Challenge de la regla para garantizar que las solicitudes incluyan un token de desafío válido. Haga esto primero en un entorno de prueba y, después, con sumo cuidado en su entorno de producción. Este enfoque tiene el potencial de bloquear a los usuarios. Por ejemplo, si la ruta de la página de registro no acepta solicitudes de texto/html `GET`, esta configuración de reglas puede bloquear eficazmente todas las solicitudes en la página de registro.

3. Habilite el registro y las métricas para la ACL web

   Según sea necesario, configure el registro, la recopilación de datos de Amazon Security Lake, el muestreo de solicitudes y CloudWatch las métricas de Amazon para la ACL web. Puede usar estas herramientas de visibilidad para monitorizar la interacción del grupo de reglas administrado de la ACFP con su tráfico.

   - Para obtener más información acerca del registro, consulte Registro del tráfico de ACL AWS WAF web.
   - Para obtener información acerca de Amazon Security Lake, consulte ¿Qué es Amazon Security Lake? y Recopilación de datos de AWS los servicios de la guía del usuario de Amazon Security Lake.
   - Para obtener información sobre CloudWatch las métricas de Amazon, consultaMonitorización con Amazon CloudWatch.
   - Para obtener información sobre cómo el muestreo de las solicitudes de web, consulte Visualizar una muestra de solicitudes web.

4. Asocie la ACL web con un recurso

   Si la ACL web aún no está asociada a un recurso de prueba, asóciela. Para obtener más información, consulte Asociar o desasociar una ACL web a un recurso AWS.

5. Supervise el tráfico y las coincidencias de las reglas de la ACFP

   Asegúrese de que el tráfico fluya normalmente y de que las reglas del grupo de reglas administrado de la ACFP agreguen etiquetas a las solicitudes web coincidentes. Puedes ver las etiquetas en los registros y ver la ACFP y las métricas de etiquetas en las métricas de Amazon CloudWatch . En los registros, las reglas que ha anulado para el recuento en el grupo de reglas aparecen en `ruleGroupList` con `action` establecida para el recuento y con `overriddenAction` indicando la acción de regla configurada que ha anulado.

6. Verificación de las capacidades de comprobación de credenciales del grupo de reglas

   Realice un intento de creación de cuentas probando las credenciales comprometidas y compruebe que el grupo de reglas coincide con ellas según lo esperado.

   a. Acceda a la página de registro de cuentas de su recurso protegido e intente agregar una cuenta nueva. Utilice el siguiente par AWS WAF de credenciales de prueba e introduzca cualquier prueba

      - Usuario: `WAF_TEST_CREDENTIAL@wafexample.com`

- Contraseña: `WAF_TEST_CREDENTIAL_PASSWORD`

Estas credenciales de prueba se clasifican como credenciales comprometidas y el grupo de reglas administrado de la ACFP agregará la etiqueta `awswaf:managed:aws:acfp:signal:credential_compromised` a la solicitud de creación de la cuenta, lo que se puede ver en los registros.

b. En los registros de la ACL web, busque la etiqueta `awswaf:managed:aws:acfp:signal:credential_compromised` en el campo `labels` de las entradas de registro de la solicitud de creación de la cuenta de prueba. Para obtener más información acerca del registro, consulte Registro del tráfico de ACL AWS WAF web.

Una vez que haya comprobado que el grupo de reglas captura las credenciales comprometidas según lo esperado, puede tomar las medidas necesarias para configurar su implementación según lo necesite para el recurso protegido.

7. En el CloudFront caso de las distribuciones, pruebe la gestión de los intentos de creación masiva de cuentas por parte del grupo de reglas

Realice esta prueba para cada criterio de respuesta satisfactoria que haya configurado para el grupo de reglas de la ACFP. Espere al menos 30 minutos entre las pruebas.

a. Para cada uno de sus criterios de éxito, identifique en la respuesta un intento de creación de cuenta que cumpla con esos criterios de éxito. A continuación, desde una sola sesión de cliente, realice al menos 5 intentos satisfactorios de creación de cuentas en menos de 30 minutos. Normalmente, un usuario solo crearía una cuenta en su sitio.

Una vez creada correctamente la primera cuenta, la regla `VolumetricSessionSuccessfulResponse` debería empezar a compararse con el resto de las respuestas de creación de cuentas, etiquetándolas y contabilizándolas, en función de la anulación de las acciones de regla. Es posible que la regla omita la primera o las dos primeras debido a la latencia.

b. En los registros de la ACL web, busque la etiqueta `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_` en el campo `labels` de las entradas de registro de las solicitudes web de creación de la cuenta de prueba. Para obtener más información acerca del registro, consulte Registro del tráfico de ACL AWS WAF web.

Estas pruebas comprueban que sus criterios de éxito coincidan con sus respuestas comprobando que los recuentos de éxitos agregados por la regla superen el umbral de la regla. Una vez alcanzado el umbral, si sigue enviando solicitudes de creación de cuentas desde la misma sesión, la regla seguirá siendo válida hasta que la tasa de éxito caiga por debajo del umbral. Si se supera el umbral, la regla compara los intentos de creación de cuentas exitosos o fallidos desde la dirección de la sesión.

8. Personalización la gestión de las solicitudes web de la ACFP

   Según sea necesario, añada sus propias reglas que permitan o bloqueen las solicitudes de forma explícita para cambiar la forma en que las reglas de la ACFP las gestionarían.

   Por ejemplo, puede utilizar las etiquetas de la ACFP para permitir o bloquear las solicitudes o para personalizar su gestión. Puede agregar una regla de coincidencia de etiquetas después del grupo de reglas administrado de la ACFP para filtrar las solicitudes etiquetadas según la gestión que desee aplicar. Tras realizar las pruebas, mantenga las reglas de la ACFP relacionadas en modo de recuento y mantenga las decisiones de gestión de las solicitudes en su regla personalizada. Para ver un ejemplo, consulte Ejemplo de ACFP: respuesta personalizada para credenciales comprometidas.

9. Elimine las reglas de prueba y active la configuración del grupo de reglas administrado de la ACFP

   Según su situación, es posible que haya decidido dejar algunas reglas de la ACFP en modo de recuento. Para las reglas que desee ejecutar tal como están configuradas dentro del grupo de reglas, deshabilite el modo de recuento en la configuración del grupo de reglas de la ACL web. Cuando termine de realizar las pruebas, también puede eliminar las reglas de coincidencia de etiquetas de prueba.

10. Monitorización y ajuste

    Para asegurarse de que las solicitudes web se gestionen como desea, monitorice de cerca el tráfico después de activar la funcionalidad de la ACFP que pretende utilizar. Ajuste el comportamiento según sea necesario con la anulación del recuento de reglas en el grupo de reglas y con sus propias reglas.

Cuando termine de probar la implementación del grupo de reglas de la ACFP, si aún no ha integrado el AWS WAF JavaScript SDK en las páginas de registro y creación de cuentas del navegador, le recomendamos encarecidamente que lo haga. AWS WAF también proporciona SDK móviles

para integrar dispositivos iOS y Android. Para obtener más información acerca de la integración de los SDK, consulte AWS WAF integración de aplicaciones cliente. Para obtener más información sobre esta recomendación, consulte Motivos por los que debería utilizar los SDK de integración de aplicaciones con ACFP.

AWS WAF Ejemplos de prevención del fraude (ACFP) en la creación de cuentas de Fraud Control

En esta sección, se muestran ejemplos de configuraciones que se adaptan a los casos de uso habituales de las implementaciones de prevención contra fraude en la creación de cuentas (ACFP) de control de fraudes de AWS WAF .

Cada ejemplo proporciona una descripción del caso de uso y, a continuación, muestra la solución en las listas JSON para las reglas configuradas de forma personalizada.

> **Note**
>
> Puede recuperar listas JSON como las que se muestran en estos ejemplos mediante el editor de reglas JSON o la descarga de JSON de la ACL web de la consola, o mediante la operación `getWebACL` en las API y la interfaz de la línea de comandos.

Temas

- Ejemplo de ACFP: configuración sencilla
- Ejemplo de ACFP: respuesta personalizada para credenciales comprometidas
- Ejemplo de ACFP: configuración de inspección de respuesta

Ejemplo de ACFP: configuración sencilla

La siguiente lista de JSON muestra un ejemplo de ACL web con un AWS WAF grupo de reglas gestionado por la prevención del fraude (ACFP) para la creación de cuentas de Fraud Control. Anote los las configuraciones adicionales `CreationPath` y `RegistrationPagePath` junto con el tipo de carga útil y la información necesaria para localizar la nueva información de la cuenta en la carga útil con el fin de verificarla. El grupo de reglas usa esta información para monitorizar y administrar sus solicitudes de creación de cuentas. Este JSON incluye la configuración generada automáticamente por la ACL web, como el espacio de nombres de las etiquetas y la URL de integración de aplicaciones de la ACL web.

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
                  "EmailField": {
                    "Identifier": "/form/email"
                  },
                  "PhoneNumberFields": [
                    {
                      "Identifier": "/form/country-code"
                    },
                    {
                      "Identifier": "/form/region-code"
                    },
                    {
                      "Identifier": "/form/phonenumber"
                    }
                  ],
```

```
                "AddressFields": [
                  {
                    "Identifier": "/form/name"
                  },
                  {
                    "Identifier": "/form/street-address"
                  },
                  {
                    "Identifier": "/form/city"
                  },
                  {
                    "Identifier": "/form/state"
                  },
                  {
                    "Identifier": "/form/zipcode"
                  }
                ]
              },
              "EnableRegexInPath": false
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
    }
  }
],
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "simpleACFP"
},
"Capacity": 50,
"ManagedByFirewallManager": false,
"LabelNamespace": "awswaf:111122223333:webacl:simpleACFP:"
}
```

Ejemplo de ACFP: respuesta personalizada para credenciales comprometidas

De forma predeterminada, la comprobación de credenciales que realiza el grupo de reglas `AWSManagedRulesACFPRuleSet` gestiona las credenciales comprometidas etiquetando la solicitud y bloqueándola. Para obtener más información sobre el grupo de reglas y el comportamiento de las reglas, consulte AWS WAF Grupo de reglas de prevención del fraude (ACFP) para la creación de cuentas de Control de Fraude.

Para informar al usuario de que las credenciales de la cuenta que ha proporcionado están comprometidas, puede hacer lo siguiente:

- Anular la regla **`SignalCredentialCompromised`** para Count: esto hace que la regla solo cuente y etiquete las solicitudes coincidentes.
- Agregar una regla de coincidencia de etiquetas con una gestión personalizada: configure esta regla para que coincida con la etiqueta de la ACFP y realice su gestión personalizada.

Las siguientes listas de la ACL web muestran el grupo de reglas administrado de la ACFP del ejemplo anterior, con la acción de regla `SignalCredentialCompromised` anulada para el recuento. Con esta configuración, cuando este grupo de reglas evalúe cualquier solicitud web que utilice credenciales comprometidas, etiquetará la solicitud, pero no la bloqueará.

Además, la ACL web ahora tiene una respuesta personalizada con el nombre `aws-waf-credential-compromised` y una nueva regla con el nombre `AccountSignupCompromisedCredentialsHandling`. La prioridad de la regla es una configuración numérica superior a la del grupo de reglas, por lo que se ejecuta después del grupo de reglas en la evaluación de la ACL web. La nueva regla hace coincidir cualquier solicitud con la etiqueta de credenciales comprometidas del grupo de reglas. Cuando la regla encuentra una coincidencia, aplica la acción Block a la solicitud con el cuerpo de la respuesta personalizada. El cuerpo de la respuesta personalizada proporciona información al usuario final de que sus credenciales se han visto comprometidas y propone una acción que tomar.

```
{
  "Name": "compromisedCreds",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/compromisedCreds/...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
```

```
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
                  "EmailField": {
                    "Identifier": "/form/email"
                  },
                  "PhoneNumberFields": [
                    {
                      "Identifier": "/form/country-code"
                    },
                    {
                      "Identifier": "/form/region-code"
                    },
                    {
                      "Identifier": "/form/phonenumber"
                    }
                  ],
                  "AddressFields": [
                    {
                      "Identifier": "/form/name"
                    },
                    {
                      "Identifier": "/form/street-address"
                    },
                    {
                      "Identifier": "/form/city"
```

```
                    },
                    {
                      "Identifier": "/form/state"
                    },
                    {
                      "Identifier": "/form/zipcode"
                    }
                  ]
                },
                "EnableRegexInPath": false
              }
            }
          ],
          "RuleActionOverrides": [
            {
              "Name": "SignalCredentialCompromised",
              "ActionToUse": {
                "Count": {}
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    },
    {
      "Name": "AccountSignupCompromisedCredentialsHandling",
      "Priority": 1,
      "Statement": {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "awswaf:managed:aws:acfp:signal:credential_compromised"
        }
      },
      "Action": {
        "Block": {
          "CustomResponse": {
```

```
            "ResponseCode": 406,
            "CustomResponseBodyKey": "aws-waf-credential-compromised",
            "ResponseHeaders": [
              {
                "Name": "aws-waf-credential-compromised",
                "Value": "true"
              }
            ]
          }
        }
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AccountSignupCompromisedCredentialsHandling"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "compromisedCreds"
  },
  "Capacity": 51,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:compromisedCreds:",
  "CustomResponseBodies": {
    "aws-waf-credential-compromised": {
      "ContentType": "APPLICATION_JSON",
      "Content": "{\n  \"credentials-compromised\": \"The credentials you provided have
 been found in a compromised credentials database.\\n\\nTry again with a different
 username, password pair.\"\n}"
    }
  }
}
```

Ejemplo de ACFP: configuración de inspección de respuesta

En la siguiente lista de JSON se muestra un ejemplo de ACL web con un AWS WAF grupo de reglas gestionado por el Control de Fraude para la creación de cuentas y prevención del fraude (ACFP) que está configurado para inspeccionar las respuestas de origen. Tenga en cuenta la configuración de inspección de respuestas, que especifica los códigos de éxito y estado de respuesta. También puede configurar los ajustes de éxito y respuesta en función de las coincidencias del JSON del encabezado,

el cuerpo y el cuerpo. Este JSON incluye la configuración generada automáticamente por la ACL web, como el espacio de nombres de las etiquetas y la URL de integración de aplicaciones de la ACL web.

> **Note**
>
> La inspección de respuestas de ATP solo está disponible en las ACL web que protegen las CloudFront distribuciones.

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
                  "EmailField": {
                    "Identifier": "/form/email"
                  },
```

```
            "PhoneNumberFields": [
              {
                "Identifier": "/form/country-code"
              },
              {
                "Identifier": "/form/region-code"
              },
              {
                "Identifier": "/form/phonenumber"
              }
            ],
            "AddressFields": [
              {
                "Identifier": "/form/name"
              },
              {
                "Identifier": "/form/street-address"
              },
              {
                "Identifier": "/form/city"
              },
              {
                "Identifier": "/form/state"
              },
              {
                "Identifier": "/form/zipcode"
              }
            ]
          },
          "ResponseInspection": {
            "StatusCode": {
              "SuccessCodes": [
                200
              ],
              "FailureCodes": [
                401
              ]
            }
          },
          "EnableRegexInPath": false
        }
      }
    ]
  }
```

```
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "simpleACFP"
  },
  "Capacity": 50,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:simpleACFP:"
  }
```

AWS WAF Control de fraudes y prevención de apropiación de cuentas (ATP)

La apropiación de cuentas es una actividad ilegal en línea en la que un atacante obtiene acceso no autorizado a la cuenta de una persona. El atacante puede hacerlo de varias formas, por ejemplo, utilizando credenciales robadas o adivinando la contraseña de la víctima mediante una serie de intentos. Cuando el atacante accede, puede robar dinero, información o servicios de la víctima. El atacante podría hacerse pasar por la víctima para acceder a otras cuentas de su propiedad o para acceder a las cuentas de otras personas u organizaciones. Además, podría intentar cambiar la contraseña del usuario para bloquear el acceso de la víctima a sus propias cuentas.

Puede monitorear y controlar los intentos de apropiación de cuentas implementando la función de prevención de apropiación de cuentas (ATP) de AWS WAF Fraud Control. AWS WAF ofrece esta función en el grupo de reglas de AWS Managed Rules `AWSManagedRulesATPRuleSet` y en los SDK complementarios de integración de aplicaciones.

El grupo de reglas administrado de ATP etiqueta y gestiona las solicitudes que podrían formar parte de intentos malintencionados de creación de cuentas. Para ello, el grupo de reglas inspecciona los intentos de inicio de sesión que los clientes envían al punto de conexión de inicio de sesión de la aplicación.

- Inspección de solicitudes: la ATP le permite ver y controlar los intentos de inicio de sesión anómalos y los intentos de inicio de sesión que utilizan credenciales robadas con el fin de evitar la apropiación de cuentas que pueda dar lugar a actividades fraudulentas. La ATP comprueba las combinaciones de correo electrónico y contraseña con su base de datos de credenciales robadas, que se actualiza periódicamente a medida que se descubren nuevas credenciales filtradas en la web oscura. La ATP agrega los datos por dirección IP y sesión de cliente para detectar y bloquear a los clientes que envían demasiadas solicitudes de naturaleza sospechosa.
- Inspección de respuestas: en el caso de CloudFront las distribuciones, además de inspeccionar las solicitudes de inicio de sesión entrantes, el grupo de reglas de la ATP inspecciona las respuestas de la aplicación a los intentos de inicio de sesión para hacer un seguimiento de las tasas de éxito y fracaso. Con esta información, la ATP puede bloquear temporalmente las sesiones de los clientes o las direcciones IP que tengan demasiados errores de inicio de sesión. AWS WAF realiza una inspección de las respuestas de forma asíncrona, por lo que no aumenta la latencia del tráfico web.

> **Note**
>
> Se le cobrarán tarifas adicionales cuando utilice este grupo de reglas administrado. Para obtener más información, consulte AWS WAF Precios.

> **Note**
>
> La característica ATP no está disponible para los grupos de usuarios de Amazon Cognito.

Temas

Componentes de la ATP

Los componentes principales de la prevención de apropiación de cuentas (ATP) de AWS WAF Fraud Control son los siguientes:

- **`AWSManagedRulesATPRuleSet`**— Las reglas de este grupo de reglas AWS administradas detectan, etiquetan y gestionan varios tipos de actividad de apropiación de cuentas. El grupo de reglas inspecciona las solicitudes web `POST` HTTP que los clientes envían al punto de conexión de inicio de sesión especificado. En el caso de CloudFront las distribuciones protegidas, el grupo de reglas también inspecciona las respuestas que la distribución envía a estas solicitudes. Para obtener una lista de los grupos de reglas, consulte AWS WAF Grupo de reglas de prevención de apropiación de cuentas (ATP) para el control del fraude. Para incluir este grupo de reglas en su ACL web, utilice una instrucción de referencia de un grupo de reglas administrado. Para obtener información acerca del uso de este grupo de reglas, consulte Adición del grupo de reglas administradas por ATP a la nueva ACL web.

  > **Note**
  >
  > Se le cobrarán tarifas adicionales cuando utilice este grupo de reglas administrado. Para obtener más información, consulte AWS WAF Precios.

- Detalles sobre las páginas de registro e inicio de sesión de su aplicación: debe proporcionar información sobre las páginas de registro cuando agregue el grupo de reglas `AWSManagedRulesATPRuleSet` a su ACL web. Esto permite que el grupo de reglas reduzca el alcance de las solicitudes que inspecciona y valide adecuadamente las credenciales de uso en las solicitudes web. El grupo de reglas de ATP funciona con nombres de usuario en formato de correo electrónico. Para obtener más información, consulte Adición del grupo de reglas administradas por ATP a la nueva ACL web.
- En el caso de CloudFront las distribuciones protegidas, detalles sobre cómo responde la aplicación a los intentos de inicio de sesión: usted proporciona detalles sobre las respuestas de la aplicación a los intentos de inicio de sesión y el grupo de reglas rastrea y administra los clientes que envían demasiados intentos de inicio de sesión fallidos. Para obtener más información acerca de cómo configurar esta opción, consulte Adición del grupo de reglas administradas por ATP a la nueva ACL web.
- JavaScript y los SDK de integración de aplicaciones móviles: implemente los SDK AWS WAF JavaScript y los SDK móviles con su implementación de ATP para habilitar el conjunto completo de capacidades que ofrece el grupo de reglas. Muchas de las reglas de la ATP utilizan la información

proporcionada por los SDK para la verificación de los clientes y la agregación del comportamiento en la sesión, necesarias para separar el tráfico de clientes legítimo del tráfico de bots. Para obtener más información sobre SDKs, consulte AWS WAF integración de aplicaciones cliente.

Puede combinar su implementación de ATP con lo siguiente para monitorizar, ajustar y personalizar sus protecciones.

- Registro y métricas: puede supervisar su tráfico y comprender cómo lo afecta el grupo de reglas gestionado por la ACFP configurando y habilitando los registros, la recopilación de datos de Amazon Security Lake y CloudWatch las métricas de Amazon para su ACL web. Las etiquetas que se `AWSManagedRulesATPRuleSet` añaden a sus solicitudes web se incluyen en los datos. Para obtener información sobre las opciones Registro del tráfico de ACL AWS WAF webMonitorización con Amazon CloudWatch, consulte y ¿Qué es Amazon Security Lake? .

  En función de sus necesidades y del tráfico que detecte, es posible que desee personalizar la implementación de `AWSManagedRulesATPRuleSet`. Por ejemplo, tal vez desee excluir parte del tráfico de la evaluación de la ATP o modificar la forma en que gestiona algunos de los intentos de apropiación de cuentas que identifica, utilizando AWS WAF funciones como las declaraciones de alcance reducido o las reglas de coincidencia de etiquetas.
- Etiquetas y reglas de coincidencia de etiquetas: para cualquiera de las reglas incluidas en `AWSManagedRulesATPRuleSet`, puede cambiar el comportamiento de bloqueo a recuento y, a continuación, compararlas con las etiquetas añadidas por las reglas. Utilice este enfoque para personalizar la forma en que gestiona las solicitudes web identificadas por el grupo de reglas administrado de ATP. Para obtener más información sobre el etiquetado y el uso de las instrucciones de coincidencia de etiquetas, consulte Instrucción de regla de coincidencia de etiquetas y AWS WAF etiquetas en las solicitudes web.
- Solicitudes y respuestas personalizadas: puede agregar encabezados personalizados a las solicitudes que permita y puede enviar respuestas personalizadas a las solicitudes que bloquee. Para ello, asocie su etiqueta coincidente con las características de solicitud y respuesta personalizadas de AWS WAF . Para obtener más información sobre cómo personalizar las solicitudes y las respuestas, consulte Solicitudes web y respuestas personalizadas en AWS WAF.

Motivos por los que debería utilizar los SDK de integración de aplicaciones con ATP

El grupo de reglas administrado de la ATP requiere los tokens de desafío que generan los SDK de integración de aplicaciones. Los tokens habilitan el conjunto completo de protecciones que ofrece el grupo de reglas.

Recomendamos encarecidamente implementar los SDK de integración de aplicaciones para un uso más eficiente del grupo de reglas de la ATP. El script de desafío debe ejecutarse antes del grupo de reglas de la ATP para que el grupo de reglas se beneficie de los tokens que adquiere el script. Esto ocurre automáticamente con los SDK de integración de aplicaciones. Si no puede utilizar los SDK, también puede configurar su ACL web de forma que ejecute la acción de regla Challenge o CAPTCHA contra todas las solicitudes que vaya a inspeccionar el grupo de reglas de la ATP. El uso de la acción de regla Challenge o CAPTCHA puede generar tarifas adicionales. Para obtener más información sobre precios, consulte precios de AWS WAF.

Capacidades del grupo de reglas de la ATP que no requieren un token

Cuando las solicitudes web no tienen un token, el grupo de reglas administrado de la ATP es capaz de bloquear los siguientes tipos de tráfico:

- Direcciones IP únicas que realizan muchas solicitudes de inicio de sesión.
- Direcciones IP únicas que realizan muchas solicitudes de inicio de sesión fallidas en un corto espacio de tiempo.
- Intentos de inicio de sesión con recorrido de contraseña, que utilizan el mismo nombre de usuario pero cambian las contraseñas.

Capacidades del grupo de reglas de ATP que requieren un token

La información proporcionada en el token de desafío amplía las capacidades del grupo de reglas y de la seguridad general de las aplicaciones cliente.

El token proporciona información del cliente con cada solicitud web, lo que permite al grupo de reglas de la ATP separar las sesiones de clientes legítimas de las sesiones de clientes que se comportan mal, incluso cuando ambas se originan en una sola dirección IP. El grupo de reglas usa la información de los tokens para agregar el comportamiento de las solicitudes de sesión de los clientes con el fin de lograr una detección y mitigación más precisas.

Cuando el token está disponible en las solicitudes web, el grupo de reglas de la ATP puede detectar y bloquear las siguientes categorías adicionales de clientes a nivel de sesión:

- Las sesiones de cliente que no superan el desafío silencioso que gestionan los SDK.
- Sesiones de clientes que utilizan nombres de usuario o contraseñas con recorrido. Esto también se conoce como “relleno de credenciales”.
- Sesiones de clientes que utilizan repetidamente credenciales robadas para el registro.
- Sesiones de clientes que pasan mucho tiempo intentando iniciar sesión.
- Sesiones de clientes que realizan muchas solicitudes de inicio de sesión. El grupo de reglas ATP proporciona un mejor aislamiento de los clientes que la regla AWS WAF basada en tasas, que puede bloquear a los clientes por dirección IP. El grupo de reglas de la ATP también utiliza un umbral inferior.
- Sesiones de clientes que realizan muchas solicitudes de inicio de sesión fallidas en poco tiempo. Esta funcionalidad está disponible para las CloudFront distribuciones protegidas de Amazon.

Para obtener más información acerca de las capacidades de este grupo de reglas, consulte AWS WAF Grupo de reglas de prevención de apropiación de cuentas (ATP) para el control del fraude.

Para obtener información sobre los SDK, consulte AWS WAF integración de aplicaciones cliente. Para obtener información sobre AWS WAF los tokens, consulteAWS WAF tokens de solicitud web. Para obtener información sobre las acciones de las reglas, consulte CAPTCHAy Challenge en AWS WAF.

Adición del grupo de reglas administradas por ATP a la nueva ACL web

Para configurar el grupo de reglas administradas de ATP y que reconozca las actividades de apropiación de cuentas en su tráfico web, debe proporcionar información sobre cómo los clientes envían las solicitudes de inicio de sesión a su aplicación. En el caso de CloudFront las distribuciones protegidas de Amazon, también debes proporcionar información sobre cómo responde tu aplicación a las solicitudes de inicio de sesión. Esta configuración se suma a la configuración normal de un grupo de reglas administrado.

Para ver la descripción del grupo de reglas y la lista de reglas, consulte AWS WAF Grupo de reglas de prevención de apropiación de cuentas (ATP) para el control del fraude.

> **Note**
>
> La base de datos de credenciales robadas de ATP solo contiene nombres de usuario en formato de correo electrónico.

Esta guía está destinada a los usuarios que, en general, saben cómo crear y administrar las ACL web, las reglas y los grupos de reglas de AWS WAF . Estos temas se tratan en secciones anteriores de esta guía. Para obtener información básica sobre cómo agregar un grupo de reglas administrado a su ACL web, consulte Adición de un grupo de reglas administrado a una ACL web a través de la consola.

Seguir las prácticas recomendadas

Utilice el grupo de reglas de ATP de acuerdo con las prácticas recomendadas de Las prácticas recomendadas para la mitigación inteligente de amenazas.

Uso del grupo de reglas de **`AWSManagedRulesATPRuleSet`** en su ACL web

1. Añada el grupo de reglas AWS gestionado `AWSManagedRulesATPRuleSet` a su ACL web y edite la configuración del grupo de reglas antes de guardarlo.

   > **Note**
   >
   > Se le cobrarán tarifas adicionales cuando utilice este grupo de reglas administrado. Para obtener más información, consulte AWS WAF Precios.

2. En el panel Configuración del grupo de reglas, proporcione la información que el grupo de reglas de ATP utiliza para inspeccionar las solicitudes de creación de cuentas.

   a. En Usar expresiones regulares en las rutas, active esta opción si quiere AWS WAF hacer coincidir las expresiones regulares con las especificaciones de las rutas de la página de inicio de sesión.

      AWS WAF admite la sintaxis de patrones utilizada por la biblioteca PCRE `libpcre` con algunas excepciones. La biblioteca está documentada en PCRE, expresiones regulares compatibles con Perl. Para obtener información sobre el AWS WAF soporte, consulteCoincidencia de patrones de expresiones regulares en AWS WAF.

   b. En el caso de la ruta de inicio de sesión, proporcione la ruta del punto de conexión de inicio de sesión de su aplicación. El grupo de reglas inspecciona solo las solicitudes HTTP de `POST` enviadas al punto de conexión que ha especificado.

> **Note**
>
> La coincidencia de puntos de conexión no distingue entre mayúsculas y minúsculas. Las especificaciones de expresiones regulares no deben incluir la marca `(?-i)`, ya que desactiva la coincidencia sin distinción entre mayúsculas y minúsculas. Las especificaciones de las cadenas deben empezar con una barra diagonal `/`.

Por ejemplo, para la URL `https://example.com/web/login`, puede proporcionar la especificación de la ruta de la cadena `/web/login`. Las rutas de las páginas de registro que comienzan con la ruta que proporcione se consideran coincidentes. Por ejemplo, `/web/login` coincide con las rutas de registro `/web/login`, `/web/login/`, `/web/loginPage` y `/web/login/thisPage`, pero no coincide con la ruta de registro `/home/web/login` o `/website/login`.

c. Para Inspeccionar solicitudes, especifique cómo acepta su aplicación los intentos de inicio de sesión. Para ello, proporcione el tipo de carga útil de la solicitud y los nombres de los campos del cuerpo de la solicitud en los que se incluyen el nombre de usuario y la contraseña. La especificación de los nombres de los campos depende del tipo de carga útil.

   - Tipo de carga útil JSON: especifique los nombres de los campos en la sintaxis del puntero JSON. Para obtener información sobre la sintaxis del puntero JSON, consulte la documentación del Grupo de trabajo de ingeniería de Internet (IETF) sobre el puntero de notación de JavaScript objetos (JSON).

     Por ejemplo, para el siguiente ejemplo de carga útil JSON, la especificación del campo de nombre de usuario es `/login/username` y la especificación del campo de contraseña es `/login/password`.

     ```
     {
         "login": {
             "username": "THE_USERNAME",
             "password": "THE_PASSWORD"
         }
     }
     ```

   - Tipo de carga útil FORM_ENCODED: use los nombres de los formularios HTML.

Por ejemplo, para un formulario HTML con elementos de entrada de usuario denominados `username1` y `password1`, la especificación del campo de nombre de usuario es `username1` y la especificación del campo de contraseña es `password1`.

d. Si estás protegiendo CloudFront las distribuciones de Amazon, en la sección Inspección de respuestas, especifica cómo indica tu aplicación el éxito o el fracaso en sus respuestas a los intentos de inicio de sesión.

> **Note**
>
> La inspección de respuestas de ATP solo está disponible en las ACL web que protegen CloudFront las distribuciones.

Especifique un único componente en la respuesta de inicio de sesión que desee que inspeccione la ATP. Para los tipos de componentes Cuerpo y JSON, AWS WAF puede inspeccionar los primeros 65 536 bytes (64 KB) del componente.

Indique sus criterios de inspección para el tipo de componente, tal y como se indica en la interfaz. Debe proporcionar los criterios de éxito y fracaso para inspeccionar el componente.

Por ejemplo, supongamos que su solicitud indica el estado de un intento de inicio de sesión en el código de estado de la respuesta y utiliza `200 OK` para indicar si se ha realizado correctamente, y `401 Unauthorized` o `403 Forbidden` si ha fallado. Debe establecer el Tipo de componente de inspección de respuesta en el Código de estado y, a continuación, en el cuadro de texto Éxito, introducir `200`, y, en el cuadro de texto Error, introducir `401` en la primera línea y `403` en la segunda.

El grupo de reglas de la ATP solo cuenta las respuestas que coinciden con sus criterios de inspección de éxito o fracaso. Las reglas del grupo de reglas actúan sobre los clientes cuando tienen una tasa de error demasiado alta entre las respuestas del recuento. Para cumplir con precisión las reglas del grupo de reglas, asegúrese de proporcionar información completa tanto para los intentos de inicio de sesión como para los fallidos.

Para ver las reglas que inspeccionan las respuestas de inicio de sesión, busque `VolumetricIpFailedLoginResponseHigh` y `VolumetricSessionFailedLoginResponseHigh` en la lista de reglas que aparece en

AWS WAF Grupo de reglas de prevención de apropiación de cuentas (ATP) para el control del fraude.

3. Proporcione cualquier configuración adicional que desee para el grupo de reglas.

   Puede limitar aún más el alcance de las solicitudes que el grupo de reglas inspecciona agregando una instrucción de restricción de acceso a la instrucción del grupo de reglas administrado. Por ejemplo, solamente puede inspeccionar las solicitudes con un argumento de consulta o una cookie específicos. El grupo de reglas inspeccionará únicamente las solicitudes `POST` HTTP enviadas al punto de conexión de inicio de sesión especificado que coincidan con los criterios de la instrucción de restricción de acceso. Para obtener información sobre las instrucciones de restricción de acceso, consulte Instrucciones de restricción de acceso.

4. Guarde los cambios en la ACL web.

Antes de implementar cambios en su ATP para el tráfico de producción, pruébelos y ajústelos en un entorno provisional o de prueba hasta que se sienta cómodo con el posible impacto en el tráfico. A continuación, pruebe y ajuste las reglas en el modo de recuento con el tráfico de producción antes de habilitarlas. Consulte la sección siguiente para obtener orientación.

Pruebas e implementación de la ATP

Esta sección proporciona una guía general para configurar y probar una implementación de prevención de apropiación de cuentas (ATP) de AWS WAF Fraud Control en su sitio. Los pasos específicos que elija seguir dependerán de sus necesidades, recursos y solicitudes web que reciba.

Esta información se suma a la información general sobre las pruebas y los ajustes que se proporcionan en Probando y ajustando sus AWS WAF protecciones.

> **Note**
>
> AWS Las reglas administradas están diseñadas para protegerlo de las amenazas web más comunes. Cuando se utilizan de acuerdo con la documentación, los grupos de reglas de reglas AWS administradas añaden otro nivel de seguridad a sus aplicaciones. Sin embargo, los grupos de reglas de reglas AWS administradas no pretenden sustituir sus responsabilidades de seguridad, que vienen determinadas por los AWS recursos que seleccione. Consulte el modelo de responsabilidad compartida para asegurarse de que sus recursos AWS estén debidamente protegidos.

> **Riesgo de tráfico de producción**
>
> Antes de implementar cambios en su ATP para el tráfico de producción, pruébelos y ajústelos en un entorno provisional o de prueba hasta que se sienta cómodo con el posible impacto en el tráfico. A continuación, pruebe y ajuste las reglas en el modo de recuento con el tráfico de producción antes de habilitarlas.

AWS WAF proporciona credenciales de prueba que puede utilizar para verificar la configuración de su ATP. En el siguiente procedimiento, configurará una ACL web de prueba para usar el grupo de reglas administrado de ATP, configurará una regla para capturar la etiqueta agregada por el grupo de reglas y, a continuación, realizará un intento de inicio de sesión con estas credenciales de prueba. Verificarás que tu ACL web ha gestionado correctamente el intento comprobando CloudWatch las métricas de Amazon para el intento de inicio de sesión.

Esta guía está destinada a los usuarios que, en general, saben cómo crear y administrar las ACL web, las reglas y los grupos de reglas de AWS WAF . Estos temas se tratan en secciones anteriores de esta guía.

Para configurar y probar una implementación de prevención de apropiación de cuentas (ATP) de AWS WAF Fraud Control

Realice estos pasos primero en un entorno de prueba y, después, en producción.

1. Agregue el grupo de reglas gestionadas para la prevención de la apropiación de cuentas (ATP) de AWS WAF Fraud Control en el modo de recuento

   > **Note**
   >
   > Se le cobrarán tarifas adicionales cuando utilice este grupo de reglas administrado. Para obtener más información, consulte AWS WAF Precios.

   Agregue el grupo de reglas AWS administradas `AWSManagedRulesATPRuleSet` a una ACL web nueva o existente y configúrelo para que no altere el comportamiento actual de la ACL web. Para obtener más información sobre las reglas y etiquetas de este grupo de reglas, consulte AWS WAF Grupo de reglas de prevención de apropiación de cuentas (ATP) para el control del fraude.

- Cuando añada el grupo de reglas administrado, edítelo y haga lo siguiente:
  - En el panel de Configuración del grupo de reglas, proporcione los detalles de las páginas de registro de su aplicación. El grupo de reglas de la ATP utiliza esta información para monitorizar las actividades de inicio de sesión. Para obtener más información, consulte Adición del grupo de reglas administradas por ATP a la nueva ACL web.
  - En el panel Reglas, abra el menú desplegable Anular todas las acciones de reglas y elija Count. Con esta configuración, AWS WAF evalúa las solicitudes comparándolas con todas las reglas del grupo de reglas y solo cuenta las coincidencias resultantes, sin dejar de agregar etiquetas a las solicitudes. Para obtener más información, consulte Invalidar acciones de reglas en un grupo de reglas.

    Con esta anulación puede supervisar el posible impacto de las reglas administradas de ATP para determinar si desea agregar excepciones, por ejemplo, excepciones para casos de uso interno.
- Sitúe el grupo de reglas de forma que se evalúe según las reglas existentes en la ACL web, con una configuración de prioridad numéricamente superior a la de cualquier regla o grupo de reglas que ya esté utilizando. Para obtener más información, consulte Procesamiento del orden de las reglas y los grupos de reglas en una ACL web.

  De esta forma, no se interrumpe su gestión actual del tráfico. Por ejemplo, si tiene reglas que detectan tráfico malicioso, como la inyección de código SQL o el scripting entre sitios, seguirán detectándolo y registrándolo. Como alternativa, si tiene reglas que permiten el tráfico no malicioso conocido, estas pueden seguir permitiéndolo sin que el grupo de reglas administrado de ATP lo bloquee. Puede decidir ajustar el procesamiento de pedidos durante sus actividades de prueba y ajuste.

2. Habilite el registro y las métricas para la ACL web

   Según sea necesario, configure el registro, la recopilación de datos de Amazon Security Lake, el muestreo de solicitudes y CloudWatch las métricas de Amazon para la ACL web. Puede usar estas herramientas de visibilidad para monitorizar la interacción del grupo de reglas administrado de ATP con su tráfico.

   - Para obtener información sobre la configuración y uso de los registros, consulte Registro del tráfico de ACL AWS WAF web.

- Para obtener información acerca de Amazon Security Lake, consulte ¿Qué es Amazon Security Lake? y Recopilación de datos de AWS los servicios de la guía del usuario de Amazon Security Lake.
- Para obtener información sobre CloudWatch las métricas de Amazon, consultaMonitorización con Amazon CloudWatch.
- Para obtener información sobre cómo el muestreo de las solicitudes de web, consulte Visualizar una muestra de solicitudes web.

3. Asocie la ACL web con un recurso

   Si la ACL web aún no está asociada a un recurso de prueba, asóciela. Para obtener más información, consulte Asociar o desasociar una ACL web a un recurso AWS.

4. Supervise el tráfico y las coincidencias de las reglas de la ATP

   Asegúrese de que el tráfico fluya normalmente y de que las reglas del grupo de reglas administrado de ATP agreguen etiquetas a las solicitudes web coincidentes. Puedes ver las etiquetas en los registros y ver las métricas de ATP y etiquetas en las CloudWatch métricas de Amazon. En los registros, las reglas que ha anulado para el recuento en el grupo de reglas aparecen en `ruleGroupList` con `action` establecida para el recuento y con `overriddenAction` indicando la acción de regla configurada que ha anulado.

5. Verificación de las capacidades de comprobación de credenciales del grupo de reglas

   Realice un intento de registro probando las credenciales comprometidas y compruebe que el grupo de reglas coincide con ellas según lo esperado.

   a. Inicie sesión en la página de inicio de sesión de su recurso protegido con el siguiente par AWS WAF de credenciales de prueba:

      - Usuario: `WAF_TEST_CREDENTIAL@wafexample.com`
      - Contraseña: `WAF_TEST_CREDENTIAL_PASSWORD`

      Estas credenciales de prueba se clasifican como credenciales comprometidas y el grupo de reglas administrado de ATP agregará la etiqueta `awswaf:managed:aws:atp:signal:credential_compromised` a la solicitud de registro, lo que se puede ver en los registros.

   b. En los registros de la ACL web, busque la etiqueta `awswaf:managed:aws:atp:signal:credential_compromised` en el campo `labels`

de las entradas de registro de las solicitudes de registro de web de prueba. Para obtener más información acerca del registro, consulte Registro del tráfico de ACL AWS WAF web.

Una vez que haya comprobado que el grupo de reglas captura las credenciales comprometidas según lo esperado, puede tomar las medidas necesarias para configurar su implementación según lo necesite para el recurso protegido.

6. Para CloudFront las distribuciones, pruebe la gestión de errores de inicio de sesión del grupo de reglas

   a. Realice esta prueba para cada criterio de respuesta al fallo que haya configurado para el grupo de reglas de la ATP. Espere al menos 10 minutos entre las pruebas.

      Para probar un único criterio de error, identifique en la respuesta un intento de inicio de sesión que no funcione con ese criterio. A continuación, desde una única dirección IP de cliente, realice al menos 10 intentos de inicio de sesión fallidos en menos de 10 minutos.

      Tras los primeros 6 errores, la regla de inicio de sesión fallido volumétrico debería empezar a coincidir con el resto de los intentos, etiquetándolos y contándolos. Es posible que la regla omita la primera o las dos primeras debido a la latencia.

   b. En los registros de la ACL web, busque la etiqueta `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high` en el campo `labels` de las entradas de registro de las solicitudes de registro de web de prueba. Para obtener más información acerca del registro, consulte Registro del tráfico de ACL AWS WAF web.

   Estas pruebas verifican que los criterios de error coincidan con las respuestas comprobando que los recuentos de inicios de sesión fallidos superen los umbrales de la regla `VolumetricIpFailedLoginResponseHigh`. Una vez alcanzado el umbral, si sigue enviando solicitudes de registro desde la misma dirección IP, la regla seguirá siendo válida hasta que la tasa de éxito caiga por debajo del umbral. Si se supera el umbral, la regla compara los intentos de registro exitosos o fallidos desde la dirección IP.

7. Personalización la gestión de las solicitudes web de la ATP

   Según sea necesario, añada sus propias reglas que permitan o bloqueen las solicitudes de forma explícita para cambiar la forma en que las reglas de la ATP las gestionarían.

Por ejemplo, puede utilizar las etiquetas de la ATP para permitir o bloquear las solicitudes o para personalizar su gestión. Puede agregar una regla de coincidencia de etiquetas después del grupo de reglas administrado de ATP para filtrar las solicitudes etiquetadas según la gestión que desee aplicar. Tras realizar las pruebas, mantenga las reglas de la ATP relacionadas en modo de recuento y mantenga las decisiones de gestión de las solicitudes en su regla personalizada. Para ver un ejemplo, consulte Ejemplo de ATP: gestión personalizada de las credenciales faltantes o comprometidas.

8. Elimine las reglas de prueba y active la configuración del grupo de reglas administrado de ATP

   Según su situación, es posible que haya decidido dejar algunas reglas de la ATP en modo de recuento. Para las reglas que desee ejecutar tal como están configuradas dentro del grupo de reglas, deshabilite el modo de recuento en la configuración del grupo de reglas de la ACL web. Cuando termine de realizar las pruebas, también puede eliminar las reglas de coincidencia de etiquetas de prueba.

9. Monitorización y ajuste

   Para asegurarse de que las solicitudes web se gestionen como desee, monitorice de cerca el tráfico después de activar la funcionalidad de la ATP que pretende utilizar. Ajuste el comportamiento según sea necesario con la anulación del recuento de reglas en el grupo de reglas y con sus propias reglas.

Cuando termine de probar la implementación del grupo de reglas de la ATP, si aún no lo ha hecho, le recomendamos encarecidamente que integre el AWS WAF JavaScript SDK en la página de inicio de sesión del navegador para mejorar las capacidades de detección. AWS WAF también proporciona SDK móviles para integrar dispositivos iOS y Android. Para obtener más información acerca de la integración de los SDK, consulte AWS WAF integración de aplicaciones cliente. Para obtener más información sobre esta recomendación, consulte Motivos por los que debería utilizar los SDK de integración de aplicaciones con ATP.

AWS WAF Ejemplos de prevención de apropiación de cuentas (ATP) en Fraud Control

En esta sección, se muestran ejemplos de configuraciones que se adaptan a los casos de uso comunes de las implementaciones de prevención contra apropiación de cuentas (ATP) del control de fraudes de AWS WAF .

Cada ejemplo proporciona una descripción del caso de uso y, a continuación, muestra la solución en las listas JSON para las reglas configuradas de forma personalizada.

> **Note**
>
> Puede recuperar listas JSON como las que se muestran en estos ejemplos mediante el editor de reglas JSON o la descarga de JSON de la ACL web de la consola, o mediante la operación `getWebACL` en las API y la interfaz de la línea de comandos.

Temas

Ejemplo de ATP: configuración sencilla

En la siguiente lista de JSON se muestra un ejemplo de ACL web con un grupo de reglas gestionado por el departamento de prevención de apropiación de cuentas (ATP) de AWS WAF Fraud Control. Tenga en cuenta la configuración adicional de la página de inicio de sesión, que proporciona al grupo de reglas la información que necesita para monitorizar y gestionar sus solicitudes de inicio de sesión. Este JSON incluye la configuración generada automáticamente por la ACL web, como el espacio de nombres de las etiquetas y la URL de integración de aplicaciones de la ACL web.

```
{
    "WebACL": {
        "LabelNamespace": "awswaf:111122223333:webacl:ATPModuleACL:",
        "Capacity": 50,
        "Description": "This is a test web ACL for ATP.",
        "Rules": [
            {
                "Priority": 1,
                "OverrideAction": {
                    "None": {}
                },
                "VisibilityConfig": {
                    "SampledRequestsEnabled": true,
                    "CloudWatchMetricsEnabled": true,
                    "MetricName": "AccountTakeOverValidationRule"
                },
                "Name": "DetectCompromisedUserCredentials",
```

```
                "Statement": {
                    "ManagedRuleGroupStatement": {
                        "VendorName": "AWS",
                        "Name": "AWSManagedRulesATPRuleSet",
                        "ManagedRuleGroupConfigs": [
                          {
                            "AWSManagedRulesATPRuleSet": {
                              "LoginPath": "/web/login",
                              "RequestInspection": {
                                "PayloadType": "JSON",
                                "UsernameField": {
                                  "Identifier": "/form/username"
                                },
                                "PasswordField": {
                                  "Identifier": "/form/password"
                                }
                              },
                              "EnableRegexInPath": false
                            }
                          }
                        ]
                    }
                }
            }
        ],
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "ATPValidationAcl"
        },
        "DefaultAction": {
            "Allow": {}
        },
        "ManagedByFirewallManager": false,
        "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
        "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
        "Name": "ATPModuleACL"
    },
    "ApplicationIntegrationURL": "https://9z87abce34ea.us-
east-1.sdk.awswaf.com/9z87abce34ea/1234567a1b10/",
    "LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}
```

Ejemplo de ATP: gestión personalizada de las credenciales faltantes o comprometidas

De forma predeterminada, las comprobaciones de credenciales que realiza el grupo de reglas `AWSManagedRulesATPRuleSet` gestionan las solicitudes web de la siguiente manera:

- Credenciales faltantes: etiqueta y bloquea la solicitud.
- Credenciales comprometidas: etiqueta la solicitud, pero no la bloquee ni la cuenta.

Para obtener más información sobre el grupo de reglas y el comportamiento de las reglas, consulte AWS WAF Grupo de reglas de prevención de apropiación de cuentas (ATP) para el control del fraude.

Puede agregar una gestión personalizada para las solicitudes web a las que les falten credenciales o estas estén comprometidas de la siguiente manera:

- Anular la regla **`MissingCredential`** para Count: esta anulación de la regla de acción hace que la regla solo cuente y etiquete las solicitudes coincidentes.
- Agregar una regla de coincidencia de etiquetas con una gestión personalizada: configure esta regla para que coincida con la etiqueta de la ATP y realice su gestión personalizada. Por ejemplo, puede redirigir al cliente a su página de registro.

Las siguientes listas muestran el grupo de reglas administrado de ATP del ejemplo anterior, con la acción de regla `MissingCredential` anulada para el recuento. Esto hace que la regla aplique su etiqueta a las solicitudes coincidentes y, a continuación, solo cuente las solicitudes, en lugar de bloquearlas.

```
"Rules": [
    {
        "Priority": 1,
        "OverrideAction": {
            "None": {}
        },
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "AccountTakeOverValidationRule"
        },
        "Name": "DetectCompromisedUserCredentials",
        "Statement": {
```

```
            "ManagedRuleGroupStatement": {
                "ManagedRuleGroupConfigs": [
                  {
                    "AWSManagedRulesATPRuleSet": {
                      "LoginPath": "/web/login",
                      "RequestInspection": {
                        "PayloadType": "JSON",
                        "UsernameField": {
                          "Identifier": "/form/username"
                        },
                        "PasswordField": {
                          "Identifier": "/form/password"
                        }
                      },
                      "EnableRegexInPath": false
                    }
                  }
                ]
                "VendorName": "AWS",
                "Name": "AWSManagedRulesATPRuleSet",
                "RuleActionOverrides": [
                  {
                    "ActionToUse": {
                      "Count": {}
                    },
                    "Name": "MissingCredential"
                  }
                ],
                "ExcludedRules": []
            }
        }
    }
],
```

Con esta configuración, cuando este grupo de reglas evalúe cualquier solicitud web que utilice credenciales perdidas o comprometidas, etiquetará la solicitud, pero no la bloqueará.

La siguiente regla tiene una configuración de prioridad numérica superior a la del grupo de reglas anterior. AWS WAF evalúa las reglas en orden numérico, empezando por el más bajo, por lo que esta regla se evaluará después de la evaluación del grupo de reglas. La regla está configurada para que coincida con cualquiera de las etiquetas de credenciales y para enviar una respuesta personalizada a las solicitudes coincidentes.

```
"Name": "redirectToSignup",
      "Priority": 10,
      "Statement": {
        "OrStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:atp:signal:missing_credential"
              }
            },
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:atp:signal:credential_compromised"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {
          "CustomResponse": {
             your custom response settings
          }
        }
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "redirectToSignup"
      }
```

Ejemplo de ATP: configuración de inspección de respuesta

En la siguiente lista de JSON se muestra un ejemplo de ACL web con un grupo de reglas gestionado por el Control de la apropiación de cuentas (ATP) para la prevención del AWS WAF fraude y configurado para inspeccionar las respuestas de origen. Tenga en cuenta la configuración de inspección de respuestas, que especifica los códigos de éxito y estado de respuesta. También puede configurar los ajustes de éxito y respuesta en función de las coincidencias del JSON del encabezado, el cuerpo y el cuerpo. Este JSON incluye la configuración generada automáticamente por la ACL

web, como el espacio de nombres de las etiquetas y la URL de integración de aplicaciones de la ACL web.

> **Note**
>
> La inspección de respuestas de ATP solo está disponible en las ACL web que protegen las CloudFront distribuciones.

```
{
    "WebACL": {
        "LabelNamespace": "awswaf:111122223333:webacl:ATPModuleACL:",
        "Capacity": 50,
        "Description": "This is a test web ACL for ATP.",
        "Rules": [
            {
                "Priority": 1,
                "OverrideAction": {
                    "None": {}
                },
                "VisibilityConfig": {
                    "SampledRequestsEnabled": true,
                    "CloudWatchMetricsEnabled": true,
                    "MetricName": "AccountTakeOverValidationRule"
                },
                "Name": "DetectCompromisedUserCredentials",
                "Statement": {
                    "ManagedRuleGroupStatement": {
                        "VendorName": "AWS",
                        "Name": "AWSManagedRulesATPRuleSet",
                        "ManagedRuleGroupConfigs": [
                          {
                            "AWSManagedRulesATPRuleSet": {
                              "LoginPath": "/web/login",
                              "RequestInspection": {
                                "PayloadType": "JSON",
                                "UsernameField": {
                                  "Identifier": "/form/username"
                                },
                                "PasswordField": {
                                  "Identifier": "/form/password"
```

```
                            }
                          },
                          "ResponseInspection": {
                            "StatusCode": {
                              "SuccessCodes": [
                                200
                              ],
                              "FailureCodes": [
                                401
                              ]
                            }
                          },
                          "EnableRegexInPath": false
                        }
                      }
                    ]
                  }
                }
            }
        ],
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "ATPValidationAcl"
        },
        "DefaultAction": {
            "Allow": {}
        },
        "ManagedByFirewallManager": false,
        "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
        "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
        "Name": "ATPModuleACL"
    },
    "ApplicationIntegrationURL": "https://9z87abce34ea.us-
east-1.sdk.awswaf.com/9z87abce34ea/1234567a1b10/",
    "LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}
```

AWS WAF Control de bots

Con el control de bots, puede monitorizar, bloquear o limitar fácilmente la tasa de los bots, como rastreadores, escáneres, monitores de estado y motores de búsqueda. Si utiliza el nivel de

inspección específico del grupo de reglas, también puede desafiar a los bots que no se identifiquen a sí mismos, lo que dificulta y encarece que los robots malintencionados operen contra su sitio web. Puede proteger sus aplicaciones utilizando solo el grupo de reglas gestionado por Bot Control o en combinación con otros grupos de reglas AWS gestionadas y sus propias reglas personalizadas. AWS WAF

El control de bots incluye un panel de control de consola que muestra qué parte del tráfico actual proviene de bots, en función del muestreo de solicitudes. Con el grupo de reglas administrado de control de bots agregado a su ACL web, puede tomar medidas contra el tráfico de bots y recibir información detallada y en tiempo real sobre el tráfico de bots más común que llega a sus aplicaciones.

> **Note**
>
> Se le cobrarán tarifas adicionales cuando utilice este grupo de reglas administrado. Para obtener más información, consulte AWS WAF Precios.

El grupo de reglas administrado de control de bots proporciona un nivel de protección básico y común que añade etiquetas a los bots que se identifican automáticamente, verifica los bots generalmente deseables y detecta las firmas de bots de alta fiabilidad. Esto le permite monitorizar y controlar las categorías comunes de tráfico de bots.

El grupo de reglas de control de bots también proporciona un nivel de protección específico que permite detectar los bots sofisticados que no se identifican a sí mismos. Todas las protecciones objetivo utilizan técnicas de detección, como la interrogación del navegador, la toma de huellas digitales y la heurística del comportamiento, para identificar el tráfico de bots inapropiado. Además, las protecciones específicas ofrecen un análisis opcional automatizado y de machine learning de las estadísticas de tráfico del sitio web para detectar actividades relacionadas con los bots. Al habilitar el machine learning, AWS WAF utiliza estadísticas sobre el tráfico del sitio web, como las marcas de tiempo, las características del navegador y la URL visitada anteriormente, para mejorar el modelo de machine learning de control de bots.

Para obtener más información acerca del grupo de reglas administradas para Control de bots, consulte AWS WAF Grupo de reglas de control de bots.

Cuando AWS WAF compara una solicitud web con el grupo de reglas gestionado por el Control de bots, el grupo de reglas añade etiquetas a las solicitudes que detecta como relacionadas con un bot, por ejemplo, la categoría y el nombre del bot. Puedes hacer coincidir estas etiquetas en tus

propias AWS WAF reglas para personalizar la gestión. Las etiquetas que genera el grupo de reglas gestionado por Bot Control se incluyen en CloudWatch las métricas de Amazon y en los registros de ACL web.

También puedes usar AWS Firewall Manager AWS WAF políticas para implementar el grupo de reglas gestionado por Bot Control en todas tus aplicaciones y en varias cuentas que formen parte de tu organización AWS Organizations.

Eventos de control de bots

Los componentes principales de la implementación de un control de bots son los siguientes:

- **`AWSManagedRulesBotControlRuleSet`**: el grupo de reglas administrado de control de bots, cuyas reglas detectan y gestionan varias categorías de bots. Este grupo de reglas añade etiquetas a las solicitudes web que detecta como tráfico de bots.

  > **Note**
  >
  > Se le cobrarán tarifas adicionales cuando utilice este grupo de reglas administrado. Para obtener más información, consulte AWS WAF Precios.

  El grupo de reglas administrado de control de bots ofrece dos niveles de protección entre los que puede elegir:

  - Común: detecta una variedad de bots que se identifican a sí mismos, como los sistemas de rastreo web, los motores de búsqueda y los navegadores automatizados. Las protecciones de control de bots de este nivel identifican los bots más comunes mediante técnicas tradicionales de detección de bots, como el análisis de datos de solicitudes estáticas. Las reglas etiquetan el tráfico de estos bots y bloquean los que no pueden verificar.
  - Objetivo: incluye las protecciones de nivel común y añade una detección dirigida para los bots sofisticados que no se identifican a sí mismos. Las protecciones específicas mitigan la actividad de los bots mediante una combinación de límites de tasas, CAPTCHA y desafíos relacionados con el navegador en segundo plano.
    - **`TGT_`**: las reglas que proporcionan una protección específica tienen nombres que comienzan por `TGT_`. Todas las protecciones específicas utilizan técnicas de detección, como la interrogación del navegador, la toma de huellas digitales y la heurística del comportamiento, para identificar el tráfico de bots inapropiado.

- **`TGT_ML_`**: las reglas de protección específicas que utilizan el machine learning tienen nombres que comienzan por `TGT_ML_`. Estas reglas utilizan un análisis automatizado y de aprendizaje automático de las estadísticas de tráfico del sitio web para detectar comportamientos anómalos indicativos de una actividad de bots distribuida y coordinada. AWS WAF analiza las estadísticas sobre el tráfico de su sitio web, como las marcas horarias, las características del navegador y la URL visitada anteriormente, para mejorar el modelo de aprendizaje automático de Bot Control. Las capacidades de machine learning están habilitadas de forma predeterminada, pero puede deshabilitarlas en la configuración de su grupo de reglas. Cuando el aprendizaje automático está desactivado, AWS WAF no evalúa estas reglas.

  Para obtener detalles, incluida la información sobre las reglas del grupo de reglas, consulte AWS WAF Grupo de reglas de control de bots.

  Para incluir este grupo de reglas en su ACL web, utilice una instrucción de referencia de un grupo de reglas administrado indicando el nivel de inspección que desea utilizar. Para el nivel objetivo, también debe indicar si desea habilitar el machine learning. Para obtener más información sobre cómo agregar este grupo de reglas administradas a su ACL web, consulte Añadir el grupo de reglas gestionado por AWS WAF Bot Control a su ACL web.

- Panel de control de bots: el panel de control de bots para su ACL web, disponible en la pestaña de control de bots de la ACL web. Use este panel de control para monitorizar su tráfico y comprender qué parte proviene de varios tipos de bots. Este puede ser un punto de partida para personalizar la administración de los bots, tal y como se describe en este tema. También puede usarlo para verificar los cambios y monitorizar la actividad de varios bots y categorías de bots.
- JavaScript y los SDK de integración de aplicaciones móviles: si utiliza el AWS WAF JavaScript nivel de protección específico del grupo de reglas de control de bots, debe implementar los SDK para dispositivos móviles. Las reglas específicas utilizan la información proporcionada por los SDK en los tokens del cliente para mejorar la detección de los bots maliciosos. Para obtener más información sobre SDKs, consulte AWS WAF integración de aplicaciones cliente.
- Registro y métricas: puede supervisar el tráfico de bots y comprender cómo el grupo de reglas gestionado por Bot Control evalúa y gestiona su tráfico estudiando los datos que los AWS WAF registros, Amazon Security Lake y Amazon CloudWatch recopilan para su ACL web. Las etiquetas que Bot Control añade a sus solicitudes web se incluyen en los datos. Para obtener información sobre estas opciones Registro del tráfico de ACL AWS WAF webMonitorización con Amazon CloudWatch, consulte y ¿Qué es Amazon Security Lake? .

En función de sus necesidades y del tráfico que detecte, es posible que desee personalizar la implementación del Control de bots. A continuación se muestran algunas opciones de uso más frecuente:

- Instrucciones de restricción de acceso: puede excluir parte del tráfico de las solicitudes web que evalúa el grupo de reglas administrado de control de bots añadiendo una instrucción de restricción de acceso dentro de la instrucción de referencia del grupo de reglas administrado de control de bots. Una instrucción de restricción de acceso puede ser cualquier instrucción de regla anidable. Cuando una solicitud no coincide con la declaración de alcance reducido, AWS WAF evalúa que no coincide con la declaración de referencia del grupo de reglas sin compararla con el grupo de reglas. Para obtener más información sobre las instrucciones de restricción de acceso, consulte Instrucciones de restricción de acceso.

  El precio del grupo de reglas administrado de control de bots aumenta en función del número de solicitudes web que AWS WAF evalúa con él. Puede ayudar a reducir estos costos utilizando una instrucción de restricción de acceso para limitar las solicitudes que evalúa el grupo de reglas. Por ejemplo, puede permitir que su página de inicio se cargue para todo el mundo, incluidos los bots, y luego aplicar las reglas del grupo de reglas a las solicitudes que se dirijan a las API de su aplicación o que contengan un tipo de contenido concreto.
- Etiquetas y reglas de coincidencia de etiquetas: puedes personalizar la forma en que el grupo de reglas de control de bots gestiona parte del tráfico de bots que identifica mediante la declaración de la regla de coincidencia de AWS WAF etiquetas. El grupo de reglas de control de bots añade etiquetas a sus solicitudes web. Puede agregar reglas de coincidencia de etiquetas después del grupo de reglas de control de bots que coincidan con las etiquetas de control de bots y aplicar la gestión que necesites. Para obtener más información sobre el etiquetado y el uso de las instrucciones de coincidencia de etiquetas, consulte Instrucción de regla de coincidencia de etiquetas y AWS WAF etiquetas en las solicitudes web.
- Solicitudes y respuestas personalizadas: puedes añadir encabezados personalizados a las solicitudes que aceptes y enviar respuestas personalizadas a las solicitudes que bloquees combinando la coincidencia de etiquetas con las funciones de solicitud y respuesta AWS WAF personalizadas. Para obtener más información sobre cómo personalizar las solicitudes y las respuestas, consulte Solicitudes web y respuestas personalizadas en AWS WAF.

Motivos por los que debería utilizar los SDK de integración de aplicaciones con el control de bots

El grupo de reglas administrado por el control de bots requiere los tokens de desafío que generan los SDK de integración de aplicaciones. Las reglas que no requieren un token de desafío en la solicitud son las protecciones de nivel común de control de bots y las reglas de nivel objetivo de machine learning. Para obtener descripciones de los niveles de protección y las reglas del grupo de reglas, consulte AWS WAF Grupo de reglas de control de bots.

Recomendamos encarecidamente implementar los SDK de integración de aplicaciones para un uso más eficiente del grupo de reglas de control de bots. El script de desafío debe ejecutarse antes del grupo de reglas del control de bots para que el grupo de reglas se beneficie de los tokens que adquiere el script.

- Con los SDK de integración de aplicaciones, el script se ejecuta automáticamente.
- Si no puede utilizar los SDK, también puede configurar su ACL web de forma que ejecute la acción de regla Challenge o CAPTCHA contra todas las solicitudes que vaya a inspeccionar el grupo de reglas de control de bots. El uso de la acción de regla Challenge o CAPTCHA puede generar tarifas adicionales. Para obtener más información sobre precios, consulte precios de AWS WAF.

Cuando implemente los SDK de integración de aplicaciones en sus clientes o utilice una de las acciones de regla que ejecuta el script de desafío, amplíe las capacidades del grupo de reglas y de la seguridad general de las aplicaciones de sus clientes.

Los tokens proporcionan información del cliente con cada solicitud web. Esta información adicional permite al grupo de reglas del control de bots separar las sesiones de clientes legítimas de las sesiones de clientes que se comportan mal, incluso cuando ambas se originan en una sola dirección IP. El grupo de reglas usa la información de los tokens para agregar el comportamiento de las solicitudes de sesión de los clientes con el fin de lograr una detección y mitigación más precisas que proporciona el nivel de protecciones específicas.

Para obtener información sobre los SDK, consulte AWS WAF integración de aplicaciones cliente. Para obtener información sobre AWS WAF los tokens, consulteAWS WAF tokens de solicitud web. Para obtener información sobre las acciones de las reglas, consulte CAPTCHAy Challenge en AWS WAF.

Añadir el grupo de reglas gestionado por AWS WAF Bot Control a su ACL web

El grupo de reglas administrado de control de bots `AWSManagedRulesBotControlRuleSet` requiere una configuración adicional para identificar el nivel de protección que se quiere implementar.

Para ver la descripción del grupo de reglas y la lista de reglas, consulte AWS WAF Grupo de reglas de control de bots.

Esta guía está destinada a los usuarios que, en general, saben cómo crear y administrar las ACL web, las reglas y los grupos de reglas de AWS WAF . Estos temas se tratan en secciones anteriores de esta guía. Para obtener información básica sobre cómo agregar un grupo de reglas administrado a su ACL web, consulte Adición de un grupo de reglas administrado a una ACL web a través de la consola.

Seguir las prácticas recomendadas

Utilice el grupo de reglas del control de bots de acuerdo con las prácticas recomendadas de Las prácticas recomendadas para la mitigación inteligente de amenazas.

Uso del grupo de reglas de **`AWSManagedRulesBotControlRuleSet`** en su ACL web

1. Agregue el grupo de reglas AWS administrado `AWSManagedRulesBotControlRuleSet` a su ACL web. Para ver la descripción completa del grupo de reglas, consulte the section called “Grupo de reglas de control de bots”.

   > **Note**
   >
   > Se le cobrarán tarifas adicionales cuando utilice este grupo de reglas administrado. Para obtener más información, consulte AWS WAF Precios.

   Cuando añada el grupo de reglas, edítelo para abrir la página de configuración del grupo de reglas.
2. En la página de configuración del grupo de reglas, en el panel Nivel de inspección, seleccione el nivel de inspección que desee usar.

   - Común: detecta una variedad de bots que se identifican a sí mismos, como los sistemas de rastreo web, los motores de búsqueda y los navegadores automatizados. Las protecciones de control de bots de este nivel identifican los bots más comunes mediante técnicas tradicionales

de detección de bots, como el análisis de datos de solicitudes estáticas. Las reglas etiquetan el tráfico de estos bots y bloquean los que no pueden verificar.

- Objetivo: incluye las protecciones de nivel común y añade una detección dirigida para los bots sofisticados que no se identifican a sí mismos. Las protecciones específicas mitigan la actividad de los bots mediante una combinación de límites de tasas, CAPTCHA y desafíos relacionados con el navegador en segundo plano.
  - **`TGT_`**: las reglas que proporcionan una protección específica tienen nombres que comienzan por `TGT_`. Todas las protecciones específicas utilizan técnicas de detección, como la interrogación del navegador, la toma de huellas digitales y la heurística del comportamiento, para identificar el tráfico de bots inapropiado.
  - **`TGT_ML_`**: las reglas de protección específicas que utilizan el machine learning tienen nombres que comienzan por `TGT_ML_`. Estas reglas utilizan un análisis automatizado y de aprendizaje automático de las estadísticas de tráfico del sitio web para detectar un comportamiento anómalo indicativo de una actividad de bots distribuida y coordinada. AWS WAF analiza las estadísticas sobre el tráfico de su sitio web, como las marcas horarias, las características del navegador y la URL visitada anteriormente, para mejorar el modelo de aprendizaje automático de Bot Control. Las capacidades de machine learning están habilitadas de forma predeterminada, pero puede deshabilitarlas en la configuración de su grupo de reglas. Cuando el aprendizaje automático está desactivado, AWS WAF no evalúa estas reglas.

3. Si utilizas el nivel de protección específico y no quieres usar el aprendizaje automático (ML) AWS WAF para analizar el tráfico web y detectar actividades distribuidas y coordinadas de bots, desactiva la opción de aprendizaje automático. El machine learning es necesario para las reglas de control de bots cuyos nombres comiencen por `TGT_ML_`. Para obtener más detalles acerca de estas reglas, consulte Listado de reglas de control de bots.
4. Agregue una instrucción de restricción de acceso para el grupo de reglas con el fin de incluir los costos de su uso. Una instrucción de restricción de acceso reduce el conjunto de solicitudes que inspecciona el grupo de reglas. Por ejemplo, en los casos de uso, comience con Ejemplo de control de bots: utilice el control de bots solo para la página de inicio de sesión y Ejemplo de control de bots: utilice el control de bots solo para contenido dinámico.
5. Proporcione cualquier configuración adicional que necesite para el grupo de reglas.
6. Guarde los cambios en la ACL web.

Antes de implementar cambios en su control de bots para el tráfico de producción, pruébelos y ajústelos en un entorno provisional o de prueba hasta que se sienta cómodo con el posible impacto

en el tráfico. A continuación, pruebe y ajuste las reglas en el modo de recuento con el tráfico de producción antes de habilitarlas. Consulte las secciones siguientes para obtener orientación.

Falsos positivos con AWS WAF Bot Control

Hemos seleccionado cuidadosamente las reglas del grupo de reglas gestionado por AWS WAF Bot Control para minimizar los falsos positivos. Comprobamos las reglas comparándolas con el tráfico global y monitorizamos su impacto en las ACL web de prueba. Sin embargo, aún es posible obtener falsos positivos debido a los cambios en los patrones de tráfico. Además, se sabe que algunos casos de uso provocan falsos positivos y requieren una personalización específica para el tráfico web.

Entre las situaciones en las que podría encontrar falsos positivos, se incluyen las siguientes:

- Las aplicaciones para móviles suelen tener agentes de usuario distintos de los navegadores, que la regla `SignalNonBrowserUserAgent` bloquea de forma predeterminada. Si espera que el tráfico provenga de aplicaciones para móviles o de cualquier otro tráfico legítimo con agentes de usuario distintos de los navegadores, tendrá que agregar una excepción para permitirlo.
- Puede confiar en un tráfico de bots específico para tareas como la supervisión del tiempo de actividad, las pruebas de integración o las herramientas de marketing. Si el control de bots identifica y bloquea el tráfico de bots que quiere permitir, tendrá que modificar la gestión añadiendo sus propias reglas. Si bien no se trata de un escenario de falso positivo para todos los clientes, si lo es para usted, tendrá que gestionarlo de la misma manera que si se tratara de un falso positivo.
- El grupo de reglas gestionado por Bot Control verifica los bots mediante las direcciones IP de. AWS WAF Si utiliza el control de bots y ha verificado bots enrutados a través de un proxy o un equilibrador de carga, debe permitirlos de forma explícita usando una regla personalizada. Para obtener información acerca de cómo crear una regla personalizada de este tipo, consulte Dirección IP reenviada.
- Una regla de control de bots con una tasa de falsos positivos global baja podría afectar gravemente a dispositivos o aplicaciones específicos. Por ejemplo, durante las pruebas y la validación, es posible que no hayamos observado solicitudes de aplicaciones con volúmenes de tráfico bajos o de navegadores o dispositivos menos habituales.
- Una regla de control de bots que tenga una tasa de falsos positivos históricamente baja podría haber aumentado el número de falsos positivos en el tráfico válido. Esto puede deberse a la aparición de nuevos patrones de tráfico o a la aparición de nuevos atributos de solicitud en el tráfico válido, lo que hace que coincidan con la regla donde no coincidía antes. Estos cambios pueden deberse a situaciones como las siguientes:

- Detalles del tráfico que se modifican a medida que el tráfico fluye a través de los dispositivos de red, como los equilibradores de carga o las redes de distribución de contenido (CDN).
- Cambios emergentes en los datos de tráfico, por ejemplo, nuevos navegadores o nuevas versiones de los navegadores existentes.

Para obtener información sobre cómo gestionar los falsos positivos que puedan derivarse del grupo de reglas administrado de control de bots de AWS WAF , consulte las instrucciones de la sección siguiente Prueba e implementación de AWS WAF Bot Control.

Prueba e implementación de AWS WAF Bot Control

En esta sección, se proporcionan instrucciones generales para configurar y probar una implementación de AWS WAF Bot Control para su sitio. Los pasos específicos que elija seguir dependerán de sus necesidades, recursos y las solicitudes web que reciba.

Esta información se suma a la información general sobre las pruebas y los ajustes que se proporcionan en Probando y ajustando sus AWS WAF protecciones.

> **Note**
>
> AWS Las reglas administradas están diseñadas para protegerlo de las amenazas web más comunes. Cuando se utilizan de acuerdo con la documentación, los grupos de reglas de reglas AWS administradas añaden otro nivel de seguridad a sus aplicaciones. Sin embargo, los grupos de reglas de reglas AWS administradas no pretenden sustituir sus responsabilidades de seguridad, que vienen determinadas por los AWS recursos que seleccione. Consulte el modelo de responsabilidad compartida para asegurarse de que sus recursos AWS estén debidamente protegidos.

> **Riesgo de tráfico de producción**
>
> Antes de implementar cambios en su control de bots para el tráfico de producción, pruébelos y ajústelos en un entorno provisional o de prueba hasta que se sienta cómodo con el posible impacto en el tráfico. A continuación, pruebe y ajuste las reglas en el modo de recuento con el tráfico de producción antes de habilitarlas.

Esta guía está destinada a los usuarios que, en general, saben cómo crear y administrar las ACL web, las reglas y los grupos de reglas de AWS WAF . Estos temas se tratan en secciones anteriores de esta guía.

Configuración y prueba de una implementación de control de bots

Realice estos pasos primero en un entorno de prueba y, después, en producción.

1. Adición del grupo de reglas administrado de control de bots

   > **Note**
   >
   > Se le cobrarán tarifas adicionales cuando utilice este grupo de reglas administrado. Para obtener más información, consulte AWS WAF Precios.

   Agregue el grupo de AWS reglas administrado `AWSManagedRulesBotControlRuleSet` a una ACL web nueva o existente y configúrelo para que no altere el comportamiento actual de la ACL web.

   - Cuando añada el grupo de reglas administrado, edítelo y haga lo siguiente:
     - En el panel Nivel de inspección, seleccione el nivel de inspección que desea utilizar.
       - Común: detecta una variedad de bots que se identifican a sí mismos, como los sistemas de rastreo web, los motores de búsqueda y los navegadores automatizados. Las protecciones de control de bots de este nivel identifican los bots más comunes mediante técnicas tradicionales de detección de bots, como el análisis de datos de solicitudes estáticas. Las reglas etiquetan el tráfico de estos bots y bloquean los que no pueden verificar.
       - Objetivo: incluye las protecciones de nivel común y añade una detección dirigida para los bots sofisticados que no se identifican a sí mismos. Las protecciones específicas mitigan la actividad de los bots mediante una combinación de límites de tasas, CAPTCHA y desafíos relacionados con el navegador en segundo plano.
         - **`TGT_`**: las reglas que proporcionan una protección específica tienen nombres que comienzan por `TGT_`. Todas las protecciones específicas utilizan técnicas de detección, como la interrogación del navegador, la toma de huellas digitales y la heurística del comportamiento, para identificar el tráfico de bots inapropiado.

- **`TGT_ML_`**: las reglas de protección específicas que utilizan el machine learning tienen nombres que comienzan por `TGT_ML_`. Estas reglas utilizan un análisis automatizado y de aprendizaje automático de las estadísticas de tráfico del sitio web para detectar comportamientos anómalos indicativos de una actividad de bots distribuida y coordinada. AWS WAF analiza las estadísticas sobre el tráfico de su sitio web, como las marcas horarias, las características del navegador y la URL visitada anteriormente, para mejorar el modelo de aprendizaje automático de Bot Control. Las capacidades de machine learning están habilitadas de forma predeterminada, pero puede deshabilitarlas en la configuración de su grupo de reglas. Cuando el aprendizaje automático está desactivado, AWS WAF no evalúa estas reglas.

  Para obtener más información sobre esta opción, consulte AWS WAF Grupo de reglas de control de bots.

- En el panel Reglas, abra el menú desplegable Anular todas las acciones de reglas y elija Count. Con esta configuración, AWS WAF evalúa las solicitudes comparándolas con todas las reglas del grupo de reglas y solo cuenta las coincidencias resultantes, sin dejar de añadir etiquetas a las solicitudes. Para obtener más información, consulte Invalidar acciones de reglas en un grupo de reglas.

  Con esta modificación, puede supervisar el posible impacto de las reglas de control de bots en su tráfico para determinar si desea agregar excepciones para casos de uso interno o para los bots deseados.

- Sitúe el grupo de reglas de forma que se evalúe según las reglas existentes en la ACL web, con una configuración de prioridad que sea numéricamente superior a la de cualquier regla o grupo de reglas que ya esté utilizando. Para obtener más información, consulte Procesamiento del orden de las reglas y los grupos de reglas en una ACL web.

  De esta forma, no se interrumpe su gestión actual del tráfico. Por ejemplo, si tiene reglas que detectan tráfico malicioso, como la inyección de código SQL o el uso de scripts entre sitios, seguirán detectando y registrando estas solicitudes. Como alternativa, si tiene reglas que permiten el tráfico no malicioso conocido, estas pueden seguir permitiéndolo sin que el grupo de reglas administrado del control de bots lo bloquee. Puede decidir ajustar el procesamiento de pedidos durante sus actividades de prueba y ajuste. Esta es una buena forma de empezar.

2. Habilite el registro y las métricas para la ACL web

Según sea necesario, configure el registro, la recopilación de datos de Amazon Security Lake, el muestreo de solicitudes y CloudWatch las métricas de Amazon para la ACL web. Puede utilizar

estas herramientas de visibilidad para supervisar la interacción del grupo de reglas gestionado por Bot Control con su tráfico.

- Para obtener más información acerca del registro, consulte Registro del tráfico de ACL AWS WAF web.
- Para obtener información acerca de Amazon Security Lake, consulte ¿Qué es Amazon Security Lake? y Recopilación de datos de AWS los servicios de la guía del usuario de Amazon Security Lake.
- Para obtener información sobre CloudWatch las métricas de Amazon, consultaMonitorización con Amazon CloudWatch.
- Para obtener información sobre cómo el muestreo de las solicitudes de web, consulte Visualizar una muestra de solicitudes web.

3. Asocie la ACL web con un recurso

   Si la ACL web aún no está asociada a un recurso, asóciela. Para obtener más información, consulte Asociar o desasociar una ACL web a un recurso AWS.

4. Supervise el tráfico y las coincidencias de las reglas del control de bots

   Asegúrese de que el tráfico fluya y de que las reglas del grupo de reglas administrado del control de bots agreguen etiquetas a las solicitudes web coincidentes. Puedes ver las etiquetas en los registros y ver las métricas de bots y etiquetas en las CloudWatch métricas de Amazon. En los registros, las reglas que ha anulado para el recuento en el grupo de reglas aparecen en `ruleGroupList` con `action` establecida para el recuento y con `overriddenAction` indicando la acción de regla configurada que ha anulado.

   > **Note**
   >
   > El grupo de reglas administrado de control de bots verifica los bots mediante las direcciones IP de AWS WAF. Si utiliza el control de bots y ha verificado bots enrutados a través de un proxy o un equilibrador de carga, debe permitirlos de forma explícita usando una regla personalizada. Para obtener información sobre cómo crear una regla personalizada, consulte Dirección IP reenviada. Para obtener información sobre cómo puede usar la regla para personalizar la gestión de las solicitudes web de control de bots, consulte el siguiente paso.

Revise detenidamente la gestión de las solicitudes web para ver si hay falsos positivos que deba mitigar con una gestión personalizada. Para ver ejemplos de falsos positivos, consulte Falsos positivos con AWS WAF Bot Control.

5. Personalización la gestión de las solicitudes web del control de bots

   Según sea necesario, añada sus propias reglas que permitan o bloqueen las solicitudes de forma explícita para cambiar la forma en que las reglas del control de bots las gestionarían.

   La forma de hacerlo depende del caso de uso, pero las siguientes son soluciones habituales:

   - Permita solicitudes de forma explícita con una regla que añada antes del grupo de reglas administrado de control de bots. De este modo, las solicitudes permitidas nunca llegan al grupo de reglas para su evaluación. Esto puede ayudar a reducir el coste de usar el grupo de reglas administrado de control de bots.
   - Excluya las solicitudes de la evaluación del control de bots añadiendo una instrucción de restricción de acceso dentro de la instrucción del grupo de reglas administrado de control de bots. Funciona igual que la opción anterior. Puede ayudar a reducir el coste de usar el grupo de reglas administrado de control de bots, ya que las solicitudes que no coinciden con la instrucción de restricción de acceso nunca llegan a la evaluación del grupo de reglas. Para obtener información sobre las instrucciones de restricción de acceso, consulte Instrucciones de restricción de acceso.

     Para ver ejemplos de , consulte lo siguiente:

     - Exclusión del rango de IP de la administración de bots
     - Permisión del tráfico de un bot que usted controla
   - Use las etiquetas de control de bots en la gestión de solicitudes para permitir o bloquear las solicitudes. Añada una regla de coincidencia de etiquetas después del grupo de reglas administrado de control de bots para filtrar las solicitudes etiquetadas que quiera permitir de las que quiera bloquear.

     Tras realizar las pruebas, mantenga las reglas del control de bots en modo de recuento y mantenga las decisiones de gestión de las solicitudes en su regla personalizada. Para obtener información sobre las instrucciones del control de bots, consulte Instrucción de regla de coincidencia de etiquetas.

     Para ver ejemplos de este tipo de personalización, consulte lo siguiente:

- Creación de una excepción para un agente de usuario bloqueado
- Permisión de un bot bloqueado específico
- Bloqueo de bots verificados

Para ver otros ejemplos, consulte AWS WAF Ejemplos de control de bots.

6. Habilite la configuración del grupo de reglas administrado de control de bots, según sea necesario.

   Según su situación, es posible que haya decidido dejar algunas reglas del control de bots en modo de recuento o con una regla de anulación diferente. Para las reglas que quiera que se ejecuten tal como están configuradas dentro del grupo de reglas, habilite la configuración de reglas normal. Para ello, edite la instrucción del grupo de reglas en su ACL web y realice los cambios en el panel Reglas.

AWS WAF Ejemplos de control de bots

En esta sección se muestran ejemplos de configuraciones que satisfacen una variedad de casos de uso comunes para las implementaciones de AWS WAF Bot Control.

Cada ejemplo proporciona una descripción del caso de uso y, a continuación, muestra la solución en las listas JSON para las reglas configuradas de forma personalizada.

> **Note**
>
> Las listas JSON que se muestran en estos ejemplos se crearon en la consola configurando la regla y, a continuación, editándola con el Editor de reglas JSON.

Temas

- Ejemplo de control de bots: configuración sencilla
- Ejemplo de control de bots: permitir explícitamente bots verificados
- Ejemplo de control de bots: bloquear bots verificados
- Ejemplo de control de bots: permitir un bot bloqueado específico
- Ejemplo de control de bots: crear una excepción para un agente de usuario bloqueado
- Ejemplo de control de bots: utilice el control de bots solo para la página de inicio de sesión

- Ejemplo de control de bots: utilice el control de bots solo para contenido dinámico
- Ejemplo de control de bots: excluir el rango de IP de la administración de bots
- Ejemplo de control de bots: permite el tráfico de un bot que tú controlas
- Ejemplo de control de bots: nivel de inspección específica
- Ejemplo de control de bots: utilice dos sentencias para limitar el uso del nivel de inspección objetivo

Ejemplo de control de bots: configuración sencilla

La siguiente lista de JSON muestra un ejemplo de ACL web con un grupo de reglas gestionado por AWS WAF Bot Control. Tenga en cuenta la configuración de visibilidad, que hace AWS WAF que se almacenen las muestras y métricas de las solicitudes con fines de supervisión.

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "Bot-WebACL",
  "Rules": [
      {
        ...
      },
      {
         "Name": "AWS-AWSBotControl-Example",
         "Priority": 5,
         "Statement": {
            "ManagedRuleGroupStatement": {
               "VendorName": "AWS",
               "Name": "AWSManagedRulesBotControlRuleSet",
               "ManagedRuleGroupConfigs": [
                 {
                   "AWSManagedRulesBotControlRuleSet": {
                     "InspectionLevel": "COMMON"
                   }
                 }
               ],
               "RuleActionOverrides": [],
               "ExcludedRules": []
```

```
            },
            "VisibilityConfig": {
               "SampledRequestsEnabled": true,
               "CloudWatchMetricsEnabled": true,
               "MetricName": "AWS-AWSBotControl-Example"
             }
          }
      }
    ],
    "VisibilityConfig": {
      ...
    },
    "Capacity": 1496,
    "ManagedByFirewallManager": false
}
```

Ejemplo de control de bots: permitir explícitamente bots verificados

AWS WAF Bot Control no bloquea los bots que se conocen como bots comunes y verificables. AWS Cuando el control de bots identifica una solicitud web como procedente de un bot verificado, añade una etiqueta con el nombre del bot y otra que indica que se trata de un bot verificado. El control de bots no añade ninguna otra etiqueta, como etiquetas de señales, para evitar que se bloqueen los bots que se sabe que funcionan correctamente.

Es posible que tengas otras AWS WAF reglas que bloqueen los bots verificados. Si quiere asegurarse de que los bots verificados están permitidos, añada una regla personalizada para permitirlos en función de las etiquetas del control de bots. La nueva regla debe ejecutarse después del grupo de reglas administrado de control de bots, de modo que las etiquetas estén disponibles para compararlas con ellas.

La siguiente regla permite explícitamente los bots verificados.

```
{
    "Name": "match_rule",
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
```

```
      "Allow": {}
    }
}
```

Ejemplo de control de bots: bloquear bots verificados

Para bloquear los bots verificados, debe agregar una regla para bloquearlos que se ejecute según el grupo de reglas administrado de control de bots de AWS WAF . Para ello, identifique los nombres de los bots que quiera bloquear y utilice una instrucción de coincidencia de etiquetas para identificarlos y bloquearlos. Si solo quiere bloquear todos los bots verificados, puede omitir la coincidencia con la etiqueta `bot:name:`.

La siguiente regla bloquea solo el bot verificado `bingbot`. Esta regla debe ejecutarse después del grupo de reglas administrado de control de bots.

```
{
    "Name": "match_rule",
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:bot:name:bingbot"
            }
          },
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:bot:verified"
            }
          }
        ]
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    }
  }
```

La siguiente regla bloquea todos los bots verificados.

```
{
    "Name": "match_rule",
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    }
}
```

Ejemplo de control de bots: permitir un bot bloqueado específico

Es posible que un bot esté bloqueado por más de una de las reglas de control de bots. Siga el procedimiento a continuación para cada regla de bloqueo.

Si una AWS WAF regla de control de bots bloquea un bot que no quieres bloquear, haz lo siguiente:

1. Compruebe los registros para identificar la regla de control de bots que bloquea el bot. La regla de bloqueo se especificará en los registros de los campos cuyos nombres comiencen por `terminatingRule`. Para obtener información acerca de la ACL web, consulte Registro del tráfico de ACL AWS WAF web. Tenga en cuenta que la etiqueta que es la regla se añade a las solicitudes.
2. En su ACL web, anule la acción de regla de bloqueo para el recuento. Para hacerlo en la consola, edite la regla del grupo de reglas de la ACL web y elija la anulación de una acción de regla Count para la regla. Esto garantiza que el bot no esté bloqueado por la regla, pero la regla seguirá aplicando su etiqueta a las solicitudes coincidentes.
3. Añada una regla de coincidencia de etiquetas a su ACL web después del grupo de reglas administrado de control de bots. Configure la regla para que coincida con la etiqueta de la regla anulada y bloquee todas las solicitudes coincidentes, excepto las del bot que no desee bloquear.

   Su ACL web ya está configurada para que el bot que desea permitir ya no esté bloqueado por la regla de bloqueo que identificó en los registros.

Compruebe de nuevo el tráfico y sus registros para asegurarse de que el bot esté autorizado a pasar. Si no es así, vuelva a realizar el procedimiento anterior.

Por ejemplo, suponga que desea bloquear todos los bots de monitorización, excepto `pingdom`. En este caso, anule la regla `CategoryMonitoring` para el recuento y, a continuación, escriba una regla para bloquear todos los bots de monitoreo, excepto los que tengan la etiqueta `pingdom` con el nombre del bot.

La siguiente regla usa el grupo de reglas administrado por el control de bots, pero anula la acción de regla para `CategoryMonitoring` para el recuento. La regla de supervisión de categorías aplica sus etiquetas como de costumbre a las solicitudes coincidentes, pero solo las cuenta en lugar de realizar su acción habitual de bloqueo.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
   "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "CategoryMonitoring"
        }
      ],
      "ExcludedRules": []
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

La siguiente regla coincide con la etiqueta de monitorización de categorías que la regla `CategoryMonitoring` anterior añade a las solicitudes web coincidentes. Entre las solicitudes de monitorización por categorías, esta regla bloquea todas excepto las que tienen una etiqueta para el nombre del bot `pingdom`.

La siguiente regla debe ejecutarse después del grupo de reglas administrado de control de bots anterior en el orden de procesamiento de las ACL web.

```
{
      "Name": "match_rule",
      "Priority": 10,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
              }
            },
            {
              "NotStatement": {
                "Statement": {
                  "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
                  }
                }
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "match_rule"
      }
}
```

Ejemplo de control de bots: crear una excepción para un agente de usuario bloqueado

Si se bloquea por error el tráfico de algunos agentes de usuario ajenos al navegador, puede crear una excepción configurando la regla de control de AWS WAF bots infractora en Recuento y, `SignalNonBrowserUserAgent` a continuación, combinando el etiquetado de la regla con sus criterios de excepción.

> **Note**
>
> Las aplicaciones para móviles suelen tener agentes de usuario distintos de los navegadores, que la regla `SignalNonBrowserUserAgent` bloquea de forma predeterminada.

La siguiente regla usa el grupo de reglas administrado por el control de bots, pero anula la acción de regla para `SignalNonBrowserUserAgent` para el recuento. La regla de señal aplica sus etiquetas como de costumbre a las solicitudes coincidentes, pero solo las cuenta en lugar de realizar su acción habitual de bloqueo.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
   "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "SignalNonBrowserUserAgent"
        }
      ],
      "ExcludedRules": []
    }
```

```
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

La siguiente regla coincide con la etiqueta de monitorización de categorías que la regla del control de bots de `SignalNonBrowserUserAgent` anterior añade a las solicitudes web coincidentes. Entre las solicitudes de señal, esta regla bloquea todas excepto las que tienen el agente de usuario que queremos permitir.

La siguiente regla debe ejecutarse después del grupo de reglas administrado de control de bots anterior en el orden de procesamiento de las ACL web.

```
{
    "Name": "match_rule",
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:signal:non_browser_user_agent"
            }
          },
          {
            "NotStatement": {
              "Statement": {
                "ByteMatchStatement": {
                  "FieldToMatch": {
                    "SingleHeader": {
                      "Name": "user-agent"
                    }
                  },
                  "PositionalConstraint": "EXACTLY",
                  "SearchString": "PostmanRuntime/7.29.2",
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
```

```
                    ]
                  }
                }
              }
            }
          ]
        }
      },
      "RuleLabels": [],
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "match_rule"
      }
}
```

Ejemplo de control de bots: utilice el control de bots solo para la página de inicio de sesión

En el siguiente ejemplo, se utiliza una sentencia de alcance reducido para aplicar el control de AWS WAF bots únicamente al tráfico que llega a la página de inicio de sesión de un sitio web, que se identifica mediante la ruta URI. `login` La ruta de URI a la página de inicio de sesión puede ser diferente a la del ejemplo, en función de la aplicación y el entorno.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
   "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
```

```
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "ByteMatchStatement": {
        "SearchString": "login",
        "FieldToMatch": {
          "UriPath": {}
        },
        "TextTransformations": [
          {
            "Priority": 0,
            "Type": "NONE"
          }
        ],
        "PositionalConstraint": "CONTAINS"
      }
    }
  }
}
```

Ejemplo de control de bots: utilice el control de bots solo para contenido dinámico

En este ejemplo, se utiliza una declaración de alcance reducido para aplicar el control de AWS WAF bots únicamente al contenido dinámico.

La instrucción de restricción de acceso excluye el contenido estático al anular los resultados de las coincidencias de un conjunto de patrones de regex:

- El conjunto de patrones de regex está configurado para coincidir con las extensiones del contenido estático. Por ejemplo, la especificación del conjunto de patrones de regex podría ser `(?i)\.(jpe?g|gif|png|svg|ico|css|js|woff2?)$`. Para obtener más información acerca de la administración de conjuntos de patrones de expresiones regulares e instrucciones , consulte Instrucción de regla de coincidencia de conjuntos de patrones de regex.
- En la instrucción de restricción de acceso, excluimos el contenido estático coincidente anidando la instrucción del conjunto de patrones de regex dentro de una instrucción `NOT`. Para obtener información sobre la instrucción de `NOT`, consulte Instrucción de reglas de NOT.

```
{
```

```
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
   "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "RegexPatternSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/regexpatternset/
excludeset/00000000-0000-0000-0000-000000000000",
            "FieldToMatch": {
              "UriPath": {}
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      }
    }
  }
}
```

Ejemplo de control de bots: excluir el rango de IP de la administración de bots

Si quieres excluir un subconjunto del tráfico web de la administración de AWS WAF Bot Control y puedes identificar ese subconjunto mediante una declaración de regla, entonces exclúyelo añadiendo una declaración de alcance reducido a la declaración del grupo de reglas gestionado por Bot Control.

La siguiente regla realiza una administración normal de los bots de control de bots en todo el tráfico web, excepto en el caso de las solicitudes web procedentes de un rango de direcciones IP específico.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "IPSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/ipset/
friendlyips/00000000-0000-0000-0000-000000000000"
          }
        }
      }
    }
```

```
  }
}
```

Ejemplo de control de bots: permite el tráfico de un bot que tú controlas

Puede configurar algunos bots de monitorización de sitios y bots personalizados para que envíen encabezados personalizados. Si quiere permitir el tráfico de estos tipos de bots, puede configurarlos para que añadan un secreto compartido en un encabezado. A continuación, puedes excluir los mensajes que tengan el encabezado añadiendo una declaración de alcance reducido a la declaración del grupo de reglas gestionado por AWS WAF Bot Control.

El siguiente ejemplo de regla excluye el tráfico con un encabezado secreto de la inspección de control de bots.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "ByteMatchStatement": {
            "SearchString": "YSBzZWNyZXQ=",
            "FieldToMatch": {
              "SingleHeader": {
```

```
                "Name": "x-bypass-secret"
              }
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ],
            "PositionalConstraint": "EXACTLY"
          }
        }
      }
    }
  }
}
```

Ejemplo de control de bots: nivel de inspección específica

Para obtener un nivel de protección mejorado, puede habilitar el nivel de inspección específico en su grupo de reglas gestionado por AWS WAF Bot Control.

En el siguiente ejemplo, las funciones de aprendizaje automático están habilitadas. Puede inhabilitar este comportamiento configurándolo `EnableMachineLearning` en`false`.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "TARGETED",
            "EnableMachineLearning": true
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
```

```
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    }
  }
}
```

Ejemplo de control de bots: utilice dos sentencias para limitar el uso del nivel de inspección objetivo

Para optimizar los costes, puede utilizar dos declaraciones de grupos de reglas gestionadas por AWS WAF Bot Control en su ACL web, con niveles y alcances de inspección independientes. Por ejemplo, podría limitar la declaración del nivel de inspección específico únicamente a los puntos finales de las aplicaciones más sensibles.

Las dos afirmaciones del siguiente ejemplo tienen un alcance que se excluye mutuamente. Sin esta configuración, una solicitud podría dar lugar a la facturación de dos evaluaciones.

> **Note**
>
> El editor visual de la `AWSManagedRulesBotControlRuleSet` consola no admite varias declaraciones que hagan referencia a ellas. En su lugar, utilice el editor JSON.

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "Bot-WebACL",
  "Rules": [
      {
        ...
      },
      {
       "Name": "AWS-AWSBotControl-Common",
       "Priority": 5,
       "Statement": {
          "ManagedRuleGroupStatement": {
             "VendorName": "AWS",
```

```
            "Name": "AWSManagedRulesBotControlRuleSet",
            "ManagedRuleGroupConfigs": [
              {
                "AWSManagedRulesBotControlRuleSet": {
                  "InspectionLevel": "COMMON"
                }
              }
            ],
            "RuleActionOverrides": [],
            "ExcludedRules": []
          },
          "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "AWS-AWSBotControl-Common"
          },
          "ScopeDownStatement": {
             "NotStatement": {
               "Statement": {
                 "ByteMatchStatement": {
                   "FieldToMatch": {
                     "UriPath": {}
                   },
                   "PositionalConstraint": "STARTS_WITH",
                   "SearchString": "/sensitive-endpoint",
                   "TextTransformations": [
                     {
                       "Type": "NONE",
                       "Priority": 0
                     }
                   ]
                 }
               }
             }
          }
        }
      },
      {
       "Name": "AWS-AWSBotControl-Targeted",
       "Priority": 6,
       "Statement": {
          "ManagedRuleGroupStatement": {
            "VendorName": "AWS",
            "Name": "AWSManagedRulesBotControlRuleSet",
```

```
            "ManagedRuleGroupConfigs": [
              {
                "AWSManagedRulesBotControlRuleSet": {
                  "InspectionLevel": "TARGETED",
                  "EnableMachineLearning": true
                }
              }
            ],
            "RuleActionOverrides": [],
            "ExcludedRules": []
          },
          "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "AWS-AWSBotControl-Targeted"
          },
          "ScopeDownStatement": {
             "Statement": {
               "ByteMatchStatement": {
                 "FieldToMatch": {
                   "UriPath": {}
                 },
                 "PositionalConstraint": "STARTS_WITH",
                 "SearchString": "/sensitive-endpoint",
                 "TextTransformations": [
                   {
                     "Type": "NONE",
                     "Priority": 0
                   }
                 ]
               }
             }
           }
        }
      }
    ],
    "VisibilityConfig": {
      ...
    },
    "Capacity": 1496,
    "ManagedByFirewallManager": false
}
```

AWS WAF integración de aplicaciones cliente

Utilice las API de integración de aplicaciones AWS WAF cliente para combinar las protecciones del lado del cliente con las protecciones AWS de ACL web del lado del servidor, a fin de comprobar que las aplicaciones cliente que envían solicitudes web a sus recursos protegidos son los clientes previstos y que sus usuarios finales son seres humanos.

Utilice las integraciones de cliente para administrar los desafíos silenciosos al navegador y los rompecabezas de CAPTCHA, obtener tokens que demuestren que el navegador y los usuarios finales han respondido satisfactoriamente, e incluir estos tokens en las solicitudes a sus puntos de conexión protegidos. Para obtener información general sobre los tokens, consulte AWS WAF . AWS WAF tokens de solicitud web

Combine las integraciones de sus clientes con las protecciones de ACL web que requieren tokens válidos para acceder a sus recursos. Puede usar grupos de reglas que comprueben y supervisen los tokens de desafíos, como los que se muestran en la siguiente sección, en Integración de amenazas inteligente y reglas administradas de AWS, y puede usar las acciones de regla CAPTCHA y Challenge para verificarlos, tal y como se describe en CAPTCHAy Challenge en AWS WAF.

AWS WAF proporciona dos niveles de integración para JavaScript las aplicaciones y uno para las aplicaciones móviles:

- Integración inteligente de amenazas: verifique la aplicación cliente y proporcione la adquisición y administración de los AWS tokens. Es similar a la funcionalidad que proporciona la acción de la AWS WAF Challenge regla. Esta funcionalidad integra completamente la aplicación cliente con el grupo de reglas `AWSManagedRulesACFPRuleSet` administrado, el grupo de reglas `AWSManagedRulesATPRuleSet` administrado y el nivel de protección objetivo del grupo de reglas `AWSManagedRulesBotControlRuleSet` administrado.

  Las API de integración de amenazas inteligentes utilizan el desafío del navegador AWS WAF silencioso para garantizar que los intentos de inicio de sesión y otras llamadas al recurso protegido solo se permitan después de que el cliente haya adquirido un token válido. Las API administran la autorización mediante token para las sesiones de las aplicaciones del cliente y recopilan información sobre el cliente para ayudar a determinar si está siendo operado por un bot o por un ser humano.

> **Note**
>
> Está disponible para JavaScript y para aplicaciones móviles Android e iOS.

- Integración de CAPTCHA: verifique a los usuarios finales con un rompecabezas de CAPTCHA personalizado que gestiona en su aplicación. Es similar a la funcionalidad que proporciona la acción de la AWS WAF CAPTCHA regla, pero con un control adicional sobre la ubicación y el comportamiento del rompecabezas.

  Esta integración aprovecha la integración JavaScript inteligente de amenazas para ejecutar desafíos silenciosos y proporcionar AWS WAF fichas a la página del cliente.

  > **Note**
  >
  > Está disponible para JavaScript las aplicaciones.

Temas

- Integración de amenazas inteligente y reglas administradas de AWS
- Acceso a las API de integración de aplicaciones AWS WAF cliente
- AWS WAF JavaScript integraciones
- AWS WAF integración de aplicaciones móviles

Integración de amenazas inteligente y reglas administradas de AWS

Las API de integración de amenazas inteligentes funcionan con las ACL web que utilizan los grupos de reglas de amenazas inteligentes para habilitar todas las funciones de estos grupos de reglas gestionados avanzados.

- AWS WAF Grupo `AWSManagedRulesACFPRuleSet` de reglas gestionado para la creación de cuentas y prevención del fraude (ACFP) para la creación de cuentas de Fraud Control.

  El fraude en la creación de cuentas es una actividad ilegal en Internet en la que un atacante crea cuentas no válidas en su solicitud para, por ejemplo, recibir bonificaciones de registro o hacerse pasar por otra persona. El grupo de reglas administrado de ACFP proporciona reglas para bloquear, etiquetar y administrar las solicitudes que podrían formar parte de intentos

malintencionados de creación de cuentas. Las API permiten verificar con precisión el navegador del cliente e información sobre la interactividad humana que las reglas de la ACFP utilizan para separar el tráfico de clientes válido del tráfico malicioso.

Para más información, consulte AWS WAF Grupo de reglas de prevención del fraude (ACFP) para la creación de cuentas de Control de Fraude y AWS WAF Control de fraude: creación de cuentas y prevención del fraude (ACFP).

- AWS WAF Grupo de reglas gestionado para la prevención de la apropiación de cuentas (ATP) para el control del fraude. `AWSManagedRulesATPRuleSet`

  La apropiación de cuentas es una actividad ilegal en línea en la que un atacante obtiene acceso no autorizado a la cuenta de una persona. El grupo de reglas administrado de la ATP proporciona reglas para bloquear, etiquetar y gestionar las solicitudes que puedan formar parte de intentos malintencionados de apropiación de cuentas. Las API permiten una verificación de clientes y una agregación de comportamientos ajustadas que las reglas de ATP utilizan para separar el tráfico de clientes válido del malicioso.

  Para más información, consulte AWS WAF Grupo de reglas de prevención de apropiación de cuentas (ATP) para el control del fraude y AWS WAF Control de fraudes y prevención de apropiación de cuentas (ATP).

- Nivel de protección específico del grupo `AWSManagedRulesBotControlRuleSet` de reglas gestionado por AWS WAF Bot Control.

  Los bots van desde los que se identifican a sí mismos y son útiles, como la mayoría de los motores de búsqueda y rastreadores, hasta los bots maliciosos que actúan contra su sitio web y no se identifican a sí mismos. El grupo de reglas administrado de control de bots proporciona reglas para supervisar, etiquetar y administrar la actividad de los bots en el tráfico web. Cuando utilice el nivel de protección específica de este grupo de reglas, las reglas específicas utilizarán la información de sesión del cliente que proporcionan las API para detectar mejor los bots maliciosos.

  Para más información, consulte AWS WAF Grupo de reglas de control de bots y AWS WAF Control de bots.

Para agregar uno de estos grupos de reglas administrados a su ACL web, consulte los procedimientos Adición del grupo de reglas administradas por ACFP a la nueva ACL web, Adición del grupo de reglas administradas por ATP a la nueva ACL web y Añadir el grupo de reglas gestionado por AWS WAF Bot Control a su ACL web.

> **Note**
>
> Los grupos de reglas administrados actualmente no bloquean las solicitudes a las que les faltan tokens. Para bloquear las solicitudes a las que les faltan tokens, después de implementar las API de integración de aplicaciones, siga las instrucciones que se indican en Bloquear solicitudes que no tienen un AWS WAF token válido.

Acceso a las API de integración de aplicaciones AWS WAF cliente

Las API de JavaScript integración están disponibles de forma general y puede usarlas para sus navegadores y otros dispositivos que las ejecuten JavaScript.

AWS WAF ofrece SDK personalizados de integración de amenazas inteligentes para aplicaciones móviles Android e iOS.

- En el caso de las aplicaciones móviles Android, AWS WAF los SDK funcionan con la API de Android versión 23 (Android versión 6) y versiones posteriores. Para obtener información sobre las versiones de Android, consulte las Notas de versión de la plataforma SDK.
- En el caso de las aplicaciones móviles de iOS, AWS WAF los SDK funcionan para la versión 13 de iOS y versiones posteriores. Para obtener información sobre las versiones de iOS, consulte las notas de la versión de iOS y iPadOS.

Acceso a las API de integración a través de la consola

1. Inicia sesión en la AWS WAF consola AWS Management Console y ábrela en https://console.aws.amazon.com/wafv2/.
2. Elija Integración de aplicaciones en el panel de navegación y, a continuación, elija la pestaña que le interese.

   - La integración inteligente de amenazas está disponible para aplicaciones móviles JavaScript y aplicaciones móviles.

     La pestaña contiene lo siguiente:

     - Una lista de las ACL web que están habilitadas para la integración de aplicaciones contra amenazas inteligentes. La lista incluye cada ACL web que utiliza el grupo de reglas administrado de `AWSManagedRulesACFPRuleSet`, el grupo de reglas administrado de `AWSManagedRulesATPRuleSet` o el nivel de protección específica del grupo de reglas

administrado de `AWSManagedRulesBotControlRuleSet`. Al implementar las API de amenazas inteligentes, utilice la URL de integración de la ACL web con la que desee realizar la integración.

- Las API a las que tiene acceso. Las JavaScript API están siempre disponibles. Para acceder a los SDK para móviles, póngase en contacto con el servicio de soporte en Contactar con AWS.

- La integración con CAPTCHA está disponible para JavaScript las aplicaciones.

  La pestaña contiene lo siguiente:

  - La URL de integración que se utilizará en la integración.
  - Las claves de API que ha creado para los dominios de las aplicaciones de sus clientes. El uso de la API de CAPTCHA requiere una clave de API cifrada que dé a los clientes el derecho a acceder a la API de AWS WAF CAPTCHA desde sus dominios. Para cada cliente con el que se integre, use una clave de API que contenga el dominio del cliente. Para obtener más información sobre estos requisitos y sobre la administración de estas claves, consulte Administración de claves de API para la API JS CAPTCHA.

AWS WAF JavaScript integraciones

Puede usar las API de JavaScript integración para implementar integraciones de AWS WAF aplicaciones en sus navegadores y otros dispositivos que se ejecuten JavaScript.

Los acertijos de CAPTCHA y los desafíos silenciosos solo se pueden ejecutar cuando los navegadores acceden a los puntos finales HTTPS. Los clientes del navegador deben ejecutarse en contextos seguros para poder adquirir los tokens.

- Las API de amenazas inteligentes le permiten gestionar la autorización de los tokens mediante un desafío silencioso al navegador del cliente e incluir los tokens en las solicitudes que envía a sus recursos protegidos.
- La API de integración de CAPTCHA se suma a las API de amenazas inteligentes y le permite personalizar la ubicación y las características del rompecabezas de CAPTCHA en las aplicaciones de sus clientes. Esta API aprovecha las API de amenazas inteligentes para adquirir tokens de AWS WAF y utilizarlos en la página una vez que el usuario final haya completado correctamente el rompecabezas de CAPTCHA.

Al utilizar estas integraciones, se asegura de que las llamadas a procedimientos remotos de su cliente contengan un token válido. Cuando estas API de integración estén instaladas en las páginas de su aplicación, podrá implementar reglas de mitigación en su ACL web, como bloquear las solicitudes que no contengan un token válido. También puede implementar reglas que impongan el uso de los tokens que obtienen las aplicaciones cliente utilizando las acciones Challenge o CAPTCHA en sus reglas.

La siguiente lista muestra los componentes básicos de una implementación típica de las API de amenazas inteligentes en una página de aplicaciones web.

```
<head>
<script type="text/javascript" src="Web ACL integration URL/challenge.js" defer></
script>
</head>
<script>
const login_response = await AwsWafIntegration.fetch(login_url, {
    method: 'POST',
    headers: {
      'Content-Type': 'application/json'
    },
    body: login_body
  });
</script>
```

La API de integración de CAPTCHA le permite personalizar la experiencia de los usuarios finales con los rompecabezas de CAPTCHA. La integración con CAPTCHA aprovecha la integración JavaScript inteligente de amenazas para la verificación del navegador y la gestión de los tokens, y añade una función para configurar y renderizar el rompecabezas del CAPTCHA.

La siguiente lista muestra los componentes básicos de una implementación típica de la API CAPTCHA JavaScript en una página de aplicación web.

```
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>

<script type="text/javascript">
    function showMyCaptcha() {
        var container = document.querySelector("#my-captcha-container");

        AwsWafCaptcha.renderCaptcha(container, {
```

```
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            ...other configuration parameters as needed...
        });
    }

    function captchaExampleSuccessFunction(wafToken) {
        // Use WAF token to access protected resources
        AwsWafIntegration.fetch("...WAF-protected URL...", {
            method: "POST",
            ...
        });
    }

    function captchaExampleErrorFunction(error) {
        /* Do something with the error */
    }
</script>

<div id="my-captcha-container">
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

Temas

- Suministro de dominios para su uso en los tokens
- Uso de la JavaScript API con políticas de seguridad de contenido
- Uso de la JavaScript API de amenazas inteligentes
- Uso de la API CAPTCHA JavaScript

Suministro de dominios para su uso en los tokens

De forma predeterminada, cuando AWS WAF crea un token, utiliza el dominio host del recurso que está asociado a la ACL web. Puede proporcionar dominios adicionales para los tokens que AWS WAF crea para las JavaScript API. Para ello, configure la `window.awsWafCookieDomainList` variable global con uno o más dominios de token.

Cuando AWS WAF crea un token, utiliza el dominio más adecuado y más corto de entre la combinación de los dominios del recurso `window.awsWafCookieDomainList` y el dominio host del recurso que está asociado a la ACL web.

Ejemplo de configuración:

```
window.awsWafCookieDomainList = ['.aws.amazon.com']
```

```
window.awsWafCookieDomainList = ['.aws.amazon.com', 'abc.aws.amazon.com']
```

No puede usar sufijos públicos en esta lista. Por ejemplo, no puede usar `gov.au` o `co.uk` como dominios de token en la lista.

Los dominios que especifique en esta lista deben ser compatibles con los demás dominios y configuraciones de dominio:

- Los dominios deben ser los que AWS WAF acepten, según el dominio host protegido y la lista de dominios simbólicos configurada para la ACL web. Para obtener más información, consulte AWS WAF Configuración de la lista de dominios del token ACL web.
- Si utilizas la API JavaScript CAPTCHA, al menos un dominio de tu clave de API de CAPTCHA debe coincidir exactamente con uno de los dominios simbólicos de uno de esos dominios simbólicos `window.awsWafCookieDomainList` o debe ser el dominio principal de uno de esos dominios simbólicos.

  Por ejemplo, para el dominio de token `mySubdomain.myApex.com`, la clave de API `mySubdomain.myApex.com` coincide exactamente y la clave de API `myApex.com` es el dominio de ápex. Cualquiera de las claves coincide con el dominio de token.

  Para obtener más información sobre las claves de API, consulte Administración de claves de API para la API JS CAPTCHA.

Si usa el grupo de reglas administrado de `AWSManagedRulesACFPRuleSet`, puede configurar un dominio que coincida con el de la ruta de creación de cuentas que proporcionó a la configuración del grupo de reglas. Para obtener más información acerca de esta configuración, consulte Adición del grupo de reglas administradas por ACFP a la nueva ACL web.

Si usa el grupo de reglas administrado de `AWSManagedRulesATPRuleSet`, debería un dominio que coincida con el de la ruta de regustri que proporcionó en la configuración del grupo de reglas. Para obtener más información acerca de esta configuración, consulte Adición del grupo de reglas administradas por ATP a la nueva ACL web.

Uso de la JavaScript API con políticas de seguridad de contenido

Si aplica políticas de seguridad de contenido (CSP) a sus recursos, para que JavaScript la implementación funcione, debe incluir en una lista de permisos el dominio AWS WAF apex. `awswaf.com` Los JavaScript SDK realizan llamadas a distintos AWS WAF puntos de conexión, por lo que permitir la inclusión de este dominio proporciona los permisos que los SDK necesitan para funcionar.

A continuación, se muestra un ejemplo de configuración para incluir en la lista de permisos el dominio de Apex: AWS WAF

```
connect-src 'self' https://*.awswaf.com;
script-src 'self' https://*.awswaf.com;
script-src-elem 'self' https://*.awswaf.com;
```

Si intentas usar los JavaScript SDK con recursos que usan CSP y no has incluido el AWS WAF dominio en la lista de permitidos, recibirás errores como los siguientes:

```
Refused to load the script ...awswaf.com/<> because it violates the following Content
 Security Policy directive: “script-src ‘self’
```

Uso de la JavaScript API de amenazas inteligentes

Las API de amenazas inteligentes proporcionan operaciones para ejecutar desafíos silenciosos contra el navegador del usuario y gestionar los AWS WAF tokens que demuestran que el desafío ha respondido satisfactoriamente y mediante CAPTCHA.

Implemente la JavaScript integración primero en un entorno de prueba y, después, en producción. Para obtener más información sobre la guía de codificación, consulta las secciones siguientes.

Uso de las API de amenazas inteligentes

1. Instalación de las API

   Si utiliza la API de CAPTCHA, puede omitir este paso. Al instalar la API de CAPTCHA, el script instala automáticamente las API de amenazas inteligentes.

   a. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

b. En el panel de navegación, elija Integración de la aplicación. En la página Integración de aplicaciones, puede ver las opciones agrupadas en pestañas.

c. Seleccione Integración de amenazas inteligentes

d. En la pestaña, seleccione la ACL web con la que desea realizar la integración. La lista incluye cada ACL web que utiliza el grupo de reglas administrado de `AWSManagedRulesACFPRuleSet`, el grupo de reglas administrado de `AWSManagedRulesATPRuleSet` o el nivel de protección objetivo del grupo de reglas administrado de `AWSManagedRulesBotControlRuleSet`.

e. Abre el panel JavaScript SDK y copia la etiqueta del script para usarla en la integración.

f. En el código de la página de la aplicación, en la sección `<head>`, inserte la etiqueta de script que copió para la ACL web. Esta inclusión hace que la aplicación cliente recupere automáticamente un token en segundo plano al cargar la página.

```
<head>
    <script type="text/javascript" src="Web ACL integration URL/challenge.js”
 defer></script>
<head>
```

Esta lista de `<script>` está configurada con el atributo `defer`, pero puede cambiarlo por otro `async` si desea un comportamiento diferente para su página.

2. (Opcional) Agrega una configuración de dominio para los tokens del cliente: de forma predeterminada, cuando AWS WAF crea un token, utiliza el dominio host del recurso que está asociado a la ACL web. Para proporcionar dominios adicionales para las JavaScript API, siga las instrucciones que se indican enSuministro de dominios para su uso en los tokens.

3. Codifique su integración de amenazas inteligentes: escriba el código para asegurarse de que la recuperación del token se complete antes de que el cliente envíe sus solicitudes a los puntos de conexión protegidos. Si ya utiliza la API `fetch` para realizar la llamada, puede sustituirla por el contenedor `fetch` de integración de AWS WAF . Si no usas la `fetch` API, puedes usar la `getToken` operación de AWS WAF integración en su lugar. Para obtener orientación sobre el código, consulte las siguientes secciones:

4. Agregue la verificación mediante token a su ACL web: añada al menos una regla a su ACL web que compruebe si hay un token de desafío válido en las solicitudes web que envíe su cliente. Puede utilizar grupos de reglas que comprueben y supervisen los tokens de desafío, como el nivel objetivo del grupo de reglas administrado de control de bots, y puede utilizar la acción de

regla Challenge para comprobarlos, tal y como se describe en CAPTCHAy Challenge en AWS WAF.

Las incorporaciones de las ACL web comprueban que las solicitudes a sus puntos de conexión protegidos incluyan el token que adquirió en la integración del cliente. Las solicitudes que incluyan un token válido y vigente pasan la inspección de Challenge y no envían otro desafío silencioso a su cliente.

5. (Opcional) Bloquee las solicitudes a las que les falten tokens: si utiliza las API con el grupo de reglas administrado de ACFP, el grupo de reglas administrado de la ATP o las reglas específicas del grupo de reglas de control de bots, estas reglas no bloquean las solicitudes a las que les falten tokens. Para bloquear las solicitudes a las que les faltan tokens, siga las instrucciones que se indican en Bloquear solicitudes que no tienen un AWS WAF token válido.

Temas

- Especificación de la API de amenazas inteligentes
- Cómo utilizar el contenedor fetch de integración
- Cómo utilizar la integración de getToken

Especificación de la API de amenazas inteligentes

En esta sección se enumeran las especificaciones de los métodos y propiedades de las JavaScript API inteligentes de mitigación de amenazas. Utilice estas API para integraciones de amenazas inteligentes y CAPTCHA.

`AwsWafIntegration.fetch()`

Envía la `fetch` solicitud HTTP al servidor mediante la implementación de AWS WAF integración.

`AwsWafIntegration.getToken()`

Recupera el AWS WAF token almacenado y lo almacena en una cookie en la página actual con su nombre `aws-waf-token` y el valor establecido en el valor del token.

`AwsWafIntegration.hasToken()`

Devuelve un booleano que indica si la cookie `aws-waf-token` contiene actualmente un token vigente.

Si también utiliza la integración de CAPTCHA, consulte las especificaciones correspondientes en Especificación de la API CAPTCHA JavaScript .

Cómo utilizar el contenedor **`fetch`** de integración

Puedes usar el AWS WAF `fetch` contenedor cambiando tus `fetch` llamadas normales a la `fetch` API en el espacio de `AwsWafIntegration` nombres. El AWS WAF contenedor admite todas las mismas opciones que la llamada a la JavaScript `fetch` API estándar y añade la gestión de los tokens para la integración. Por lo general, este enfoque es la forma más sencilla de integrar su aplicación.

Antes de la implementación del contenedor

La siguiente lista de ejemplos muestra el código estándar antes de implementar el contenedor `AwsWafIntegration fetch`.

```
const login_response = await fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
     },
     body: login_body
   });
```

Después de la implementación del contenedor

La siguiente lista muestra el mismo código con la implementación del contenedor `AwsWafIntegration fetch`.

```
const login_response = await AwsWafIntegration.fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
     },
     body: login_body
   });
```

Cómo utilizar la integración de **`getToken`**

AWS WAF requiere que sus solicitudes a los puntos finales protegidos incluyan la cookie nombrada `aws-waf-token` con el valor de su token actual.

La operación de `getToken` es una llamada a la API asíncrona que recupera el token de AWS WAF y lo almacena en una cookie en la página actual con el nombre `aws-waf-token`, y el valor establecido al valor del token. Puede usar esta cookie de token en su página según sea necesario.

Cuando se llama a `getToken`, hace lo siguiente:

- Si un token vigente ya está disponible, la llamada lo devuelve inmediatamente.
- De lo contrario, la llamada recupera un nuevo token del proveedor de tokens y espera hasta 2 segundos a que se complete el flujo de trabajo de adquisición del token antes de que se agote el tiempo de espera. Si se agota el tiempo de espera de la operación, se generará un error que deberá gestionar su código de llamada.

La operación `getToken` viene acompañada de una operación `hasToken` que indica si la cookie `aws-waf-token` contiene actualmente un token que no ha caducado.

`AwsWafIntegration.getToken()`recupera un token válido y lo almacena como una cookie. La mayoría de las llamadas de los clientes adjuntan automáticamente esta cookie, pero algunas no. Por ejemplo, las llamadas realizadas entre dominios anfitriones no adjuntan la cookie. En los detalles de implementación que aparecen a continuación, mostramos cómo trabajar con ambos tipos de llamadas de clientes.

`getToken`Implementación básica, para llamadas que adjuntan la **`aws-waf-token`** cookie

La siguiente lista de ejemplos muestra el código estándar para implementar la operación `getToken` con una solicitud de inicio de sesión.

```
const login_response = await AwsWafIntegration.getToken()
     .catch(e => {
         // Implement error handling logic for your use case
     })
     // The getToken call returns the token, and doesn't typically require special
 handling
     .then(token => {
         return loginToMyPage()
     })

 async function loginToMyPage() {
     // Your existing login code
 }
```

Envío del formulario solo después de que el token esté disponible en **`getToken`**

La siguiente lista muestra cómo registrar un oyente de eventos para interceptar los envíos de formularios hasta que haya un token válido disponible para su uso.

```
<body>
   <h1>Login</h1>
   <p></p>
   <form id="login-form" action="/web/login" method="POST" enctype="application/x-www-
form-urlencoded">
     <label for="input_username">USERNAME</label>
     <input type="text" name="input_username" id="input_username"><br>
     <label for="input_password">PASSWORD</label>
     <input type="password" name="input_password" id="input_password"><br>
     <button type="submit">Submit<button>
   </form>

 <script>
   const form = document.querySelector("#login-form");

   // Register an event listener to intercept form submissions
   form.addEventListener("submit", (e) => {
       // Submit the form only after a token is available
       if (!AwsWafIntegration.hasToken()) {
           e.preventDefault();
           AwsWafIntegration.getToken().then(() => {
               e.target.submit();
           }, (reason) => { console.log("Error:"+reason) });
         }
     });
 </script>
 </body>
```

Adjuntar el token cuando el cliente no adjunta la **`aws-waf-token`** cookie de forma predeterminada

`AwsWafIntegration.getToken()`recupera un token válido y lo almacena como una cookie, pero no todas las llamadas a los clientes adjuntan esta cookie de forma predeterminada. Por ejemplo, las llamadas realizadas entre dominios anfitriones no adjuntan la cookie.

El `fetch` contenedor maneja estos casos automáticamente, pero si no puedes usar el `fetch` contenedor, puedes manejarlo usando un encabezado personalizado`x-aws-waf-token`. AWS

WAF lee los símbolos de este encabezado, además de leerlos de la `aws-waf-token` cookie. El código siguiente muestra un ejemplo de cómo configurar el encabezado.

```
const token = await AwsWafIntegration.getToken();
const result = await fetch('/url', {
    headers: {
        'x-aws-waf-token': token,
    },
});
```

De forma predeterminada, AWS WAF solo acepta los tokens que contienen el mismo dominio que el dominio host solicitado. Cualquier token multidominio requiere las entradas correspondientes en la lista de dominios del token de ACL web. Para obtener más información, consulte AWS WAF Configuración de la lista de dominios del token ACL web.

Para obtener información adicional sobre el uso de los tokens entre dominios, consulte aws-waf-bot-controlaws-samples/ -. api-protection-with-captcha

Uso de la API CAPTCHA JavaScript

La JavaScript API de CAPTCHA le permite configurar el rompecabezas de CAPTCHA y colocarlo donde desee en su aplicación cliente. Esta API aprovecha las funciones de las JavaScript API de amenazas inteligentes para adquirir y utilizar los AWS WAF tokens una vez que el usuario final haya completado satisfactoriamente un rompecabezas de CAPTCHA.

Implemente la JavaScript integración primero en un entorno de prueba y, después, en producción. Para obtener más información sobre la guía de codificación, consulta las secciones siguientes.

Uso de la API de integración de CAPTCHA

1. Instalación de la API

    a. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.

    b. En el panel de navegación, elija Integración de la aplicación. En la página Integración de aplicaciones, puede ver las opciones agrupadas en pestañas.

    c. Seleccione la Integración de CAPTCHA.

    d. Copie la etiqueta del script de JavaScript integración que aparece en la lista para utilizarla en la integración.

e. En el código de la página de la aplicación, en la sección `<head>`, inserte la etiqueta de script que copió. Esta inclusión hace que el rompecabezas de CAPTCHA esté disponible para su configuración y uso.

```
<head>
    <script type="text/javascript" src="integrationURL/jsapi.js" defer></
script>
</head>
```

Esta lista de `<script>` está configurada con el atributo `defer`, pero puede cambiarlo por otro `async` si desea un comportamiento diferente para su página.

El script de CAPTCHA también carga automáticamente el script de integración de amenazas inteligentes si aún no está presente. El script de integración de amenazas inteligentes hace que la aplicación cliente recupere automáticamente un token en segundo plano al cargar la página y proporciona otras funciones de administración de tokens que necesita para usar la API de CAPTCHA.

2. (Opcional) Agregue una configuración de dominio para los tokens del cliente: de forma predeterminada, cuando AWS WAF crea un token, utiliza el dominio host del recurso que está asociado a la ACL web. Para proporcionar dominios adicionales para las JavaScript API, siga las instrucciones que se indican enSuministro de dominios para su uso en los tokens.
3. Obtenga la clave de API cifrada del cliente: la API de CAPTCHA requiere una clave de API cifrada que contenga una lista de dominios de cliente válidos. AWS WAF usa esta clave para comprobar que el dominio de cliente que utilizas con la integración está aprobado para usar AWS WAF CAPTCHA. Para generar su clave de API, siga las instrucciones que se indican en Administración de claves de API para la API JS CAPTCHA.
4. Codifique la implementación del widget de CAPTCHA: implemente la llamada a la API `renderCaptcha()` en su página, en la ubicación en la que quiera usarla. Para obtener información acerca de cómo configurar y usar esta función, consulte las siguientes secciones, Especificación de la API CAPTCHA JavaScript y Cómo renderizar el rompecabezas de CAPTCHA.

   La implementación del CAPTCHA se integra con las API de integración inteligente de amenazas para gestionar los tokens y ejecutar llamadas de búsqueda que utilizan los tokens. AWS WAF Para obtener orientación sobre el uso de estas API, consulte Uso de la JavaScript API de amenazas inteligentes.

5. Agregue la verificación mediante token a su ACL web: añada al menos una regla a su ACL web que compruebe si hay un token de CAPTCHA válido en las solicitudes web que envíe su cliente. Puede utilizar la acción de regla CAPTCHA para realizar la comprobación, tal y como se describe en CAPTCHAy Challenge en AWS WAF.

   Las incorporaciones de las ACL web comprueban que las solicitudes que van a sus puntos de conexión protegidos incluyen el token que adquirió en la integración con el cliente. Las solicitudes que incluyen un token de CAPTCHA válido y vigente pasan la inspección de acción de regla CAPTCHA y no presentan al usuario final otro rompecabezas de CAPTCHA.

Temas

- Especificación de la API CAPTCHA JavaScript
- Cómo renderizar el rompecabezas de CAPTCHA
- Gestión de una respuesta CAPTCHA de AWS WAF
- Administración de claves de API para la API JS CAPTCHA

Especificación de la API CAPTCHA JavaScript

En esta sección se enumeran las especificaciones de los métodos y propiedades de las API de JavaScript CAPTCHA. Utilice las JavaScript API de CAPTCHA para ejecutar rompecabezas de CAPTCHA personalizados en sus aplicaciones cliente.

Esta API se basa en las API de amenazas inteligentes, que se utilizan para configurar y gestionar la adquisición y el uso de los AWS WAF tokens. Consulte Especificación de la API de amenazas inteligentes.

`AwsWafCaptcha.renderCaptcha(container, configuration)`

Presenta un rompecabezas de AWS WAF CAPTCHA al usuario final y, en caso de éxito, actualiza el token del cliente con la validación del CAPTCHA. Esto solo está disponible con la integración de CAPTCHA. Utilice esta llamada junto con las API de amenazas inteligentes para gestionar la recuperación de los tokens y proporcionarlos en sus llamadas `fetch`. Para usar las API de amenazas inteligentes en Especificación de la API de amenazas inteligentes.

A diferencia del intersticial de CAPTCHA que se AWS WAF envía, el rompecabezas de CAPTCHA renderizado con este método muestra el rompecabezas inmediatamente, sin una pantalla de título inicial.

`container`

El objeto `Element` para el elemento contenedor objetivo de la página. Por lo general, se recupera llamando a `document.getElementById()` o `document.querySelector()`.

Obligatorio: sí

Tipo: `Element`

configuración

Un objeto que contiene los ajustes de configuración de CAPTCHA, de la siguiente manera:

`apiKey`

La clave de API cifrada que habilita los permisos para el dominio del cliente. Utilice la consola AWS WAF para generar las claves de API para los dominios de los clientes. Puede utilizar una clave para hasta cinco dominios. Para obtener más información, consulte Administración de claves de API para la API JS CAPTCHA.

Obligatorio: sí

Tipo: `string`

`onSuccess: (wafToken: string) => void;`

Se llama con un AWS WAF token válido cuando el usuario final completa correctamente un rompecabezas de CAPTCHA. Utilice el token en las solicitudes que envíe a los puntos finales que proteja con una AWS WAF ACL web. El token proporciona la prueba y la marca de tiempo de la última vez que se ha completado con éxito el rompecabezas.

Obligatorio: sí

`onError?: (error: CaptchaError) => void;`

Se llama con un objeto de error cuando se produce un error durante la operación de CAPTCHA.

Obligatorio: no

Definición de clase **`CaptchaError`**: el controlador `onError` proporciona un tipo de error con la siguiente definición de clase.

```
CaptchaError extends Error {
```

```
    kind: "internal_error" | "network_error" | "token_error" | "client_error";
    statusCode?: number;
}
```

- `kind`: el tipo de error devuelto.
- `statusCode`: el código de estado HTTP, si está disponible. Lo utiliza `network_error` si el error se debe a un error HTTP.

`onLoad?: () => void;`

Se llama cuando se carga un nuevo rompecabezas de CAPTCHA.

Obligatorio: no

`onPuzzleTimeout?: () => void;`

Se llama cuando un rompecabezas de CAPTCHA no se completa antes de que caduque.

Obligatorio: no

`onPuzzleCorrect?: () => void;`

Se llama cuando se proporciona una respuesta correcta a un rompecabezas de CAPTCHA.

Obligatorio: no

`onPuzzleIncorrect?: () => void;`

Se llama cuando se proporciona una respuesta incorrecta a un rompecabezas de CAPTCHA.

Obligatorio: no

`defaultLocale`

La configuración regional predeterminada que se utilizará en el rompecabezas de CAPTCHA. Las instrucciones escritas para los rompecabezas de CAPTCHA están disponibles en árabe (ar-SA), chino simplificado (zh-CN), holandés (nl-NL), inglés (en-US), francés (fr-FR), alemán (de-DE), italiano (it-IT), japonés (ja-JP), portugués brasileño (pt-BR), español (es-ES) y turco (tr-TR). Las instrucciones de audio están disponibles en todos los idiomas escritos, excepto en chino y japonés, que por defecto son el inglés. Para cambiar el idioma predeterminado, proporciona el idioma internacional y el código de configuración regional, por ejemplo,`ar-SA`.

Predeterminado: el idioma que se utiliza actualmente en el navegador del usuario final

Obligatorio: no

Tipo: `string`

`disableLanguageSelector`

Si se establece en `true`, el rompecabezas de CAPTCHA oculta el selector de idioma.

Valor predeterminado: `false`

Obligatorio: no

Tipo: `boolean`

`dynamicWidth`

Si se establece en `true`, el rompecabezas de CAPTCHA cambia de ancho para que sea compatible con el ancho de la ventana del navegador.

Valor predeterminado: `false`

Obligatorio: no

Tipo: `boolean`

`skipTitle`

Si se establece en `true`, el rompecabezas de CAPTCHA no mostrará el título del rompecabezas Resuelva el rompecabezas.

Valor predeterminado: `false`

Obligatorio: no

Tipo: `boolean`

Cómo renderizar el rompecabezas de CAPTCHA

Puede usar la AWS WAF `renderCaptcha` llamada donde desee en la interfaz de cliente. La llamada recupera un acertijo de CAPTCHA AWS WAF, lo renderiza y envía los resultados para su verificación. AWS WAF Al realizar la llamada, proporciona la configuración de renderización del rompecabezas y las devoluciones de llamadas que desea ejecutar cuando los usuarios finales

completen el rompecabezas. Para obtener detalles sobre las opciones, consulte la sección anterior, Especificación de la API CAPTCHA JavaScript .

Utilice esta llamada junto con la funcionalidad de administración de tokens de las API de integración de amenazas inteligentes. Esta llamada proporciona a su cliente un token que verifica que ha completado correctamente el rompecabezas de CAPTCHA. Utilice las API de integración de amenazas inteligentes para gestionar el token y proporcionarlo en las llamadas de sus clientes a los puntos finales protegidos con ACL web. AWS WAF Para obtener más información acerca de las API de amenazas inteligentes, consulte Uso de la JavaScript API de amenazas inteligentes.

Despliegue de ejemplo

La siguiente lista de ejemplos muestra una implementación de CAPTCHA estándar, incluida la ubicación de la URL de AWS WAF integración en la sección. `<head>`

En este listado, se configura la función `renderCaptcha` con una devolución de llamada de éxito que utiliza el contenedor `AwsWafIntegration.fetch` de las API de integración de amenazas inteligentes. Para obtener información acerca de esta función, consulte Cómo utilizar el contenedor `fetch` de integración.

```
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>

<script type="text/javascript">
    function showMyCaptcha() {
        var container = document.querySelector("#my-captcha-container");

        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            ...other configuration parameters as needed...
        });
    }

    function captchaExampleSuccessFunction(wafToken) {
        // Captcha completed. wafToken contains a valid WAF token. Store it for
        // use later or call AwsWafIntegration.fetch() to use it easily.
        // It will expire after a time, so calling AwsWafIntegration.getToken()
        // again is advised if the token is needed later on, outside of using the
        // fetch wrapper.
```

```
        // Use WAF token to access protected resources
        AwsWafIntegration.fetch("...WAF-protected URL...", {
            method: "POST",
            headers: {
                "Content-Type": "application/json",
            },
            body: "{ ... }" /* body content */
        });
    }

    function captchaExampleErrorFunction(error) {
        /* Do something with the error */
    }
</script>

<div id="my-captcha-container">
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

Ejemplo de configuración

En la siguiente lista de ejemplos, se muestra la configuración no predeterminada de `renderCaptcha` para las opciones de ancho y título.

```
        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            dynamicWidth: true,
            skipTitle: true
        });
```

Para obtener información completa acerca de las opciones de configuración, consulte Especificación de la API CAPTCHA JavaScript .

Gestión de una respuesta CAPTCHA de AWS WAF

Una AWS WAF regla con una CAPTCHA acción finaliza la evaluación de una solicitud web coincidente si la solicitud no tiene un token con una marca de tiempo de CAPTCHA válida. Si la solicitud es una llamada de texto/html `GET`, la acción CAPTCHA envía al cliente un intersticial con

un rompecabezas de CAPTCHA. Si no integras la JavaScript API de CAPTCHA, el intersticial resuelve el rompecabezas y, si el usuario final lo resuelve correctamente, vuelve a enviar la solicitud automáticamente.

Al integrar la JavaScript API de CAPTCHA y personalizar el manejo del CAPTCHA, es necesario detectar la respuesta de CAPTCHA que termina, entregar el CAPTCHA personalizado y, a continuación, si el usuario final resuelve el acertijo con éxito, volver a enviar la solicitud web del cliente.

El siguiente ejemplo de código muestra cómo hacerlo.

> **Note**
>
> La respuesta de AWS WAF CAPTCHA acción tiene un código de estado HTTP 405, que utilizamos para reconocer la respuesta en este código. CAPTCHA Si su punto de conexión protegido utiliza un código de estado HTTP 405 para comunicar cualquier otro tipo de respuesta para la misma llamada, este código de ejemplo también renderizará un rompecabezas de CAPTCHA para esas respuestas.

```
<!DOCTYPE html>
<html>
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>
<body>
    <div id="my-captcha-box"></div>
    <div id="my-output-box"></div>

    <script type="text/javascript">
    async function loadData() {
        // Attempt to fetch a resource that's configured to trigger a CAPTCHA
        // action if the rule matches. The CAPTCHA response has status=HTTP 405.
        const result = await AwsWafIntegration.fetch("/protected-resource");

        // If the action was CAPTCHA, render the CAPTCHA and return

        // NOTE: If the endpoint you're calling in the fetch call responds with HTTP
 405
        // as an expected response status code, then this check won't be able to tell
 the
```

```
        // difference between that and the CAPTCHA rule action response.

        if (result.status === 405) {
            const container = document.querySelector("#my-captcha-box");
            AwsWafCaptcha.renderCaptcha(container, {
                apiKey: "...API key goes here...",
                onSuccess() {
                    // Try loading again, now that there is a valid CAPTCHA token
                    loadData();
                },
            });
            return;
        }

        const container = document.querySelector("#my-output-box");
        const response = await result.text();
        container.innerHTML = response;
    }

    window.addEventListener("load", () => {
        loadData();
    });
    </script>
</body>
</html>
```

Administración de claves de API para la API JS CAPTCHA

Para integrar AWS WAF CAPTCHA en una aplicación cliente con la JavaScript API, necesitas la etiqueta de integración de la JavaScript API y la clave de API cifrada del dominio del cliente en el que quieres ejecutar el rompecabezas de CAPTCHA.

La integración de la aplicación CAPTCHA JavaScript utiliza las claves de API cifradas para comprobar que el dominio de la aplicación cliente tiene permiso para utilizar la API de CAPTCHA. AWS WAF Cuando llamas a la API de CAPTCHA desde tu JavaScript cliente, proporcionas una clave de API con una lista de dominios que incluye un dominio para el cliente actual. Puedes enumerar hasta 5 dominios en una sola clave cifrada.

Requisitos de la clave de API

La clave de API que utilices en su integración de CAPTCHA debe contener un dominio que se aplique al cliente en el que utilice la clave.

- Si especifica una `window.awsWafCookieDomainList` en la integración de amenazas inteligentes del cliente, al menos un dominio de la clave de API debe coincidir exactamente con uno de los dominios de token en `window.awsWafCookieDomainList` o debe ser el dominio de ápex de uno de esos dominios de token.

  Por ejemplo, para el dominio de token `mySubdomain.myApex.com`, la clave de API `mySubdomain.myApex.com` coincide exactamente y la clave de API `myApex.com` es el dominio de ápex. Cualquiera de las claves coincide con el dominio de token.

  Para obtener información sobre la configuración de la lista de dominios de tokens, consulte Suministro de dominios para su uso en los tokens.
- De lo contrario, el dominio actual debe estar incluido en la clave de API. El dominio actual es el dominio que puede ver en la barra de direcciones del navegador.

Los dominios que utilice deben ser los que AWS WAF acepten, según el dominio host protegido y la lista de dominios simbólicos configurada para la ACL web. Para obtener más información, consulte AWS WAF Configuración de la lista de dominios del token ACL web.

¿Cómo elegir la región para tu clave de API

AWS WAF puede generar claves de API de CAPTCHA en cualquier región en la que estén AWS WAF disponibles.

Como regla general, debe usar la misma región para su clave de API de CAPTCHA que usa para su ACL web. Sin embargo, si esperas una audiencia global para una ACL web regional, puedes obtener una etiqueta de JavaScript integración de CAPTCHA con un alcance específico CloudFront y una clave de API con un alcance específico CloudFront, y utilizarlas con una ACL web regional. Este enfoque permite a los clientes cargar un rompecabezas de CAPTCHA desde la región más cercana a ellos, lo que reduce la latencia.

Las claves de la API de CAPTCHA que están dirigidas a otras regiones no CloudFront se admiten para su uso en varias regiones. Solo se pueden usar en la región a la que están destinadas.

Cómo generar una clave de API para los dominios de sus clientes

Para obtener la URL de integración y generar y recuperar las claves de API a través de la consola.

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

2. En el panel de navegación, elija Integración de la aplicación.
3. En el panel de ACL web que están habilitadas para la integración de aplicaciones, selecciona la región que deseas usar como clave de API. También puede seleccionar la región en el panel de claves de API de la pestaña de integración con CAPTCHA.
4. Seleccione la pestaña Integración de CAPTCHA. Esta pestaña proporciona la etiqueta de JavaScript integración CAPTCHA, que puede usar en su integración, y la lista de claves de API. Ambas se refieren a la región seleccionada.
5. En el panel de Claves de API, seleccione Generar claves. Aparecerá el cuadro de diálogo de generación de claves.
6. Introduzca los dominios de cliente que desee incluir en la clave. Puede especificar una máximo de 5. Cuando haya terminado, elija Generar clave. La interfaz vuelve a la pestaña de integración de CAPTCHA, donde aparece la nueva clave.

   Una vez creada, la clave de API es inmutable. Si necesita realizar cambios en una clave, genere una nueva clave y úsela en su lugar.
7. (Opcional) Copia la clave recién generada para usarla en la integración.

Para este trabajo, también puedes usar las API REST o uno de los AWS SDK específicos del idioma. Las llamadas a la API REST son CreateApiKey y ListApiKeys.

Para eliminar una clave de API

Para eliminar una clave de API, debes usar la API REST o uno de los AWS SDK específicos del idioma. La llamada a la API REST es DeleteApiKey. No puedes usar la consola para eliminar una clave.

Tras eliminar una clave, pueden pasar hasta 24 horas hasta AWS WAF que no se permita su uso en todas las regiones.

AWS WAF integración de aplicaciones móviles

Puede utilizar los SDK AWS WAF móviles para implementar SDK de integración de amenazas AWS WAF inteligentes para aplicaciones móviles Android e iOS.

- En el caso de las aplicaciones móviles de Android, los AWS WAF SDK funcionan para la versión 23 de la API de Android (versión 6 de Android) y versiones posteriores. Para obtener información sobre las versiones de Android, consulte las Notas de versión de la plataforma SDK.

- En el caso de las aplicaciones móviles de iOS, AWS WAF los SDK funcionan para la versión 13 de iOS y versiones posteriores. Para obtener información sobre las versiones de iOS, consulte las notas de la versión de iOS y iPadOS.

Con el SDK para móviles, puede gestionar la autorización de los tokens e incluirlos en las solicitudes que envíe a sus recursos protegidos. Al utilizar los SDK, se asegura de que las llamadas a procedimientos remotos de su cliente contengan un token válido. Además, cuando estas integración esté instalada en las páginas de su aplicación, podrá implementar reglas de mitigación en su ACL web, como bloquear las solicitudes que no contengan un token válido.

Para acceder a los SDK para móviles, póngase en contacto con el servicio de soporte en Contactar con AWS.

> **Note**
>
> Los SDK AWS WAF móviles no están disponibles para la personalización de CAPTCHA.

El enfoque básico para usar el SDK consiste en crear un proveedor de fichas mediante un objeto de configuración y, a continuación, utilizar el proveedor de fichas para recuperar las fichas. AWS WAF De forma predeterminada, el proveedor de tokens incluye los tokens recuperados en sus solicitudes web para su recurso protegido.

La siguiente es una lista parcial de la implementación de un SDK, en la que se muestran los componentes principales. Para obtener más ejemplos más detallados, consulte Escribir el código para el SDK AWS WAF móvil.

iOS

```
let url: URL = URL(string: "Web ACL integration URL")!
 let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
 "Domain name")
 let tokenProvider = WAFTokenProvider(configuration)
 let token = tokenProvider.getToken()
```

Android

```
URL applicationIntegrationURL = new URL("Web ACL integration URL");
```

```
String domainName = "Domain name";
WAFConfiguration configuration =
WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
configuration);
WAFToken token = tokenProvider.getToken();
```

Instalación del SDK AWS WAF móvil

Para acceder a los SDK para móviles, póngase en contacto con el servicio de soporte en Contactar con AWS.

Implemente SDK para móviles primero en un entorno de prueba y, después, en producción.

Para instalar el SDK AWS WAF móvil

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, elija Integración de la aplicación.
3. En la pestaña Integraciones de amenazas inteligentes, haga lo siguiente:
   a. En el panel ACL web que están habilitadas para la integración de aplicaciones, busque la ACL web con la que se esté integrando. Copie y guarde la URL de integración de la ACL web para utilizarla en la implementación. También puede obtener esta URL a través de la llamada a la API `GetWebACL`.
   b. Elija el tipo y la versión del dispositivo móvil y, a continuación, seleccione Descargar. Puedes elegir la versión que desees, pero te recomendamos que utilices la versión más reciente. AWS WAF descarga el `zip` archivo para su dispositivo en su ubicación de descarga estándar.
4. En su entorno de desarrollo de aplicaciones, descomprima el archivo en la ubicación de trabajo que elija. En el directorio de nivel superior del archivo zip, busque y abra el `README`. Sigue las instrucciones del `README` archivo para instalar el SDK AWS WAF móvil y usarlo en el código de tu aplicación móvil.
5. Programe la aplicación de acuerdo con las instrucciones que se detallan en las siguientes secciones.

La especificación del SDK AWS WAF móvil

En esta sección, se enumeran los objetos, las operaciones y los ajustes de configuración del SDK para la última versión disponible del SDK para móviles de AWS WAF . Para obtener información detallada sobre cómo funcionan el proveedor de tokens y las operaciones para las distintas combinaciones de ajustes de configuración, consulte Cómo funciona el SDK AWS WAF móvil.

`WAFToken`

Contiene un AWS WAF token.

`getValue()`

Recupera la representación `String` del valor `WAFToken`.

`WAFTokenProvider`

Administra los tokens en su aplicación para móviles. Implemente esto usando un objeto `WAFConfiguration`.

`getToken()`

Si la actualización en segundo plano está habilitada, devuelve el token almacenado en caché. Si la actualización en segundo plano está desactivada, se realiza una llamada síncrona y bloqueante AWS WAF a para recuperar un nuevo token.

`onTokenReady(WAFTokenResultCallback)`

Indica al proveedor de tokens que actualice el token e invoque la devolución de llamada proporcionada cuando haya un token activo listo. El proveedor de tokens invocará la devolución de llamada en un hilo en segundo plano cuando el token esté en caché y esté listo. Llame a esto cuando la aplicación se cargue por primera vez y también cuando vuelva a un estado activo. Para obtener más información sobre cómo volver a un estado activo, consulte the section called “Recuperación de un token tras la inactividad de la aplicación”.

Para las aplicaciones de Android o iOS, puede configurar `WAFTokenResultCallback` en la operación que desee que el proveedor de tokens invoque cuando el token solicitado esté listo. Su implementación de `WAFTokenResultCallback` debe tomar los parámetros `WAFToken`, `SdkError`. Para las aplicaciones de iOS, también puede crear una función en línea.

`storeTokenInCookieStorage(WAFToken)`

Le indica `WAFTokenProvider` que almacene el AWS WAF token especificado en el administrador de cookies del SDK. De forma predeterminada, el token solo se agrega

al almacén de cookies cuando se adquiere por primera vez y cuando se actualiza. Si la aplicación borra el almacén de cookies compartido por cualquier motivo, el SDK no volverá a añadir el AWS WAF token automáticamente hasta la próxima actualización.

`WAFConfiguration`

Contiene la configuración para la implementación de `WAFTokenProvider`. Al implementar esto, debe proporcionar la URL de integración de la ACL web, el nombre de dominio que se utilizará en el token y cualquier configuración no predeterminada que desee que utilice el proveedor de tokens.

La siguiente lista especifica los ajustes de configuración que puede administrar en el objeto `WAFConfiguration`.

`applicationIntegrationUrl`

La URL de integración de aplicaciones. Consíguelo desde la AWS WAF consola o mediante una llamada a la `getWebACL` API.

Obligatorio: sí

Tipo: URL específica de la aplicación. Para iOS, consulte URL de iOS. Para Android, consulte URL java.net.

`backgroundRefreshEnabled`

Indica si desea que el proveedor de tokens actualice el token en segundo plano. Si lo establece, el proveedor de tokens los actualiza en segundo plano de acuerdo con los ajustes de configuración que rigen las actividades de actualización automática de los tokens.

Obligatorio: no

Tipo: `Boolean`

Valor predeterminado: `TRUE`

`domainName`

El dominio que se utilizará en el token, que se utiliza para la adquisición de tokens y el almacenamiento de cookies. Por ejemplo, `example.com` o `aws.amazon.com`. Suele ser el dominio del host de su recurso que está asociado a la ACL web, al que enviará las solicitudes web. En el caso del grupo de reglas administrado de la

ACFP, `AWSManagedRulesACFPRuleSet`, este suele ser un dominio único que coincide con el dominio de la ruta de creación de cuentas que proporcionó en la configuración del grupo de reglas. En el caso del grupo de reglas administrado de ATP, `AWSManagedRulesATPRuleSet`, este suele ser un dominio único que coincide con el dominio de la ruta de inicio de sesión que proporcionó en la configuración del grupo de reglas.

No se admiten sufijos públicos. Por ejemplo, no puede usar `gov.au` o `co.uk` como dominio de token.

El dominio debe ser uno que AWS WAF acepte, según el dominio host protegido y la lista de dominios simbólicos de la ACL web. Para obtener más información, consulte AWS WAF Configuración de la lista de dominios del token ACL web.

Obligatorio: sí

Tipo: `String`

`maxErrorTokenRefreshDelayMsec`

El tiempo máximo en milisegundos para esperar antes de repetir una actualización del token después de un intento fallido. Este valor se utiliza cuando la recuperación del token ha fallado y se ha vuelto a intentar `maxRetryCount` veces.

Obligatorio: no

Tipo: `Integer`

Valor predeterminado: `5000` (5 segundos)

Valor mínimo permitido: `1` (1 milisegundo)

Valor máximo permitido: `30000` (30 segundos)

`maxRetryCount`

El número máximo de reintentos que se pueden realizar con un retroceso exponencial cuando se solicita un token.

Obligatorio: no

Tipo: `Integer`

Valor predeterminado: si la actualización en segundo plano está habilitada, `5`. De lo contrario, `3`.

Valor mínimo permitido: `0`

Valor máximo permitido: `10`

`setTokenCookie`

Indique si desea que el administrador de cookies del SDK agregue una cookie de token en sus solicitudes. De forma predeterminada, esto añade una cookie de token a todas las solicitudes. El administrador de cookies agrega una cookie de token a cualquier solicitud cuya ruta esté por debajo de la ruta especificada en `tokenCookiePath`.

Obligatorio: no

Tipo: `Boolean`

Valor predeterminado: `TRUE`

`tokenCookiePath`

Se usa cuando `setTokenCookie` es `TRUE`. Indica la ruta de nivel superior en la que desea que el gestor de cookies del SDK añada una cookie de token. El administrador agrega una cookie de token a todas las solicitudes que envíe a esta ruta y a todas las rutas secundarias.

Por ejemplo, si lo establece en `/web/login`, el administrador incluirá la cookie de token para todo lo que se envíe a `/web/login` y para cualquiera de sus rutas secundarias, como `/web/login/help`. No incluye el token para las solicitudes enviadas a otras rutas, como `/`, `/web` o `/web/order`.

Obligatorio: no

Tipo: `String`

Valor predeterminado: `/`

`tokenRefreshDelaySec`

Se utiliza para la actualización en segundo plano. La cantidad máxima de tiempo en segundos entre las actualizaciones del token en segundo plano.

Obligatorio: no

Tipo: `Integer`

Valor predeterminado: 88

Valor mínimo permitido: 88

Valor máximo permitido: `300` (5 minutos)

Cómo funciona el SDK AWS WAF móvil

Los SDK para móviles le proporcionan un proveedor de tokens configurable que puede usar para recuperar y usar los tokens. El proveedor de los tokens verifica que las solicitudes que permita procedan de clientes legítimos. Cuando envías solicitudes a los AWS recursos con los que proteges AWS WAF, incluyes el token en una cookie para validar la solicitud. Puede gestionar la cookie de token manualmente o dejar que el proveedor de tokens lo haga por usted.

En esta sección se describen las interacciones entre las clases, las propiedades y los métodos que se incluyen en el SDK para móviles. Para obtener información sobre la especificación del SDK, consulte La especificación del SDK AWS WAF móvil.

Recuperación de tokens y almacenamiento en caché

Cuando crea la instancia del proveedor de tokens en su aplicación para móviles, configura la forma en que quiere que administre los tokens y su recuperación. Su principal opción es cómo mantener los tokens válidos y vigentes para usarlos en las solicitudes web de su aplicación:

- Actualización en segundo plano habilitada Es el valor predeterminado. El proveedor del token actualiza automáticamente el token en segundo plano y lo guarda en caché. Con la actualización en segundo plano habilitada, cuando llama `getToken()`, la operación recupera el token almacenado en caché.

  El proveedor de tokens actualiza el token a intervalos configurables, de modo que siempre haya un token vigente en la memoria caché mientras la aplicación esté activa. La actualización en segundo plano se detiene mientras la aplicación está inactiva. Para obtener información acerca de este tema, consulte Recuperación de un token tras la inactividad de la aplicación.
- Actualización en segundo plano desactivada: puede deshabilitar la actualización de los tokens en segundo plano y, a continuación, recuperarlos solo cuando lo solicite. Los tokens recuperados bajo demanda no se almacenan en caché y, si lo desea, puede recuperar más de uno. Cada token es independiente de los demás que recupere y cada uno tiene su propia marca de tiempo que se utiliza para calcular el vencimiento.

Dispone de las siguientes opciones para recuperar el token cuando la actualización en segundo plano está desactivada:

- **`getToken()`**— Cuando llamas `getToken()` con la actualización en segundo plano desactivada, la llamada recupera un nuevo token de forma sincrónica. AWS WAF Se trata de una llamada que puede bloquear y que puede afectar a la capacidad de respuesta de la aplicación si se invoca en el hilo principal.
- **`onTokenReady(WAFTokenResultCallback)`**: esta llamada recupera de forma asíncrona un nuevo token y, a continuación, invoca la devolución de llamada resultante proporcionada en un hilo en segundo plano cuando el token está listo.

Cómo reintenta el proveedor de tokens las recuperaciones de tokens fallidas

El proveedor de tokens vuelve a intentar recuperar el token automáticamente cuando se produce un error en la recuperación. Los reintentos se realizan inicialmente mediante un retroceso exponencial con un tiempo de espera de reintento inicial de 100 ms. Para obtener información acerca de las recuperaciones exponenciales, consulte Reintentos de error y retroceso exponencial en AWS.

Cuando el número de reintentos alcanza el valor `maxRetryCount` configurado, el proveedor de tokens deja de intentarlo o pasa a intentarlo cada `maxErrorTokenRefreshDelayMsec` milisegundos, según el tipo de recuperación del token:

- **`onTokenReady()`**: el proveedor de tokens pasa a esperar `maxErrorTokenRefreshDelayMsec` milisegundos entre intentos y continúa intentando recuperar el token.
- Actualización en segundo plano: el proveedor del token pasa a esperar `maxErrorTokenRefreshDelayMsec` milisegundos entre intentos y continúa intentando recuperar el token.
- Llamadas **`getToken()`** bajo demanda, cuando la actualización en segundo plano está desactivada: el proveedor de tokens deja de intentar recuperar un token y devuelve el valor del token anterior o un valor nulo si no hay ningún token anterior.

Recuperación de un token tras la inactividad de la aplicación

La actualización en segundo plano solo se realiza mientras la aplicación se considera activa para el tipo de aplicación:

- iOS: la actualización en segundo plano se realiza cuando la aplicación está en primer plano.

- Android: la actualización en segundo plano se realiza cuando la aplicación no está cerrada, ya sea en primer plano o en segundo plano.

Si la aplicación permanece en un estado que no admite la actualización en segundo plano durante más de los `tokenRefreshDelaySec` segundos configurados, el proveedor de tokens detiene la actualización en segundo plano. Por ejemplo, en el caso de una aplicación de iOS, si `tokenRefreshDelaySec` es 300 y la aplicación se cierra o pasa a segundo plano durante más de 300 segundos, el proveedor de tokens deja de actualizar el token. Cuando la aplicación vuelve a un estado activo, el proveedor de tokens reinicia automáticamente la actualización en segundo plano.

Cuando su aplicación vuelva a estar activa, llame a `onTokenReady()` para recibir una notificación cuando el proveedor de tokens recupere y almacene en caché un nuevo token. No se limites a llamar a `getToken()`, ya que es posible que la caché aún no contenga un token válido actual.

Escribir el código para el SDK AWS WAF móvil

Esta sección se brinda ejemplos de códigos para usar el SDK para móviles.

Inicialización del proveedor de tokens y obtención de tokens

La instancia del proveedor de tokens se inicia mediante un objeto de configuración. A continuación, puede recuperar los tokens mediante las operaciones disponibles. Se indican a continuación los componentes básicos del código exigido.

iOS

```
let url: URL = URL(string: "Web ACL integration URL")!
let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
 "Domain name")
let tokenProvider = WAFTokenProvider(configuration)

//onTokenReady can be add as an observer for
 UIApplication.willEnterForegroundNotification
self.tokenProvider.onTokenReady() { token, error in
 if let token = token {
 //token available
 }

 if let error = error {
 //error occurred after exhausting all retries
 }
}
```

```
//getToken()
let token = tokenProvider.getToken()
```

Android

Ejemplo de Java:

```
String applicationIntegrationURL = "Web ACL integration URL";
//Or
URL applicationIntegrationURL = new URL("Web ACL integration URL");

String domainName = "Domain name";

WAFConfiguration configuration =
 WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
 configuration);

// implement a token result callback
WAFTokenResultCallback callback = (wafToken, error) -> {
 if (wafToken != null) {
 // token available
 } else {
 // error occurred in token refresh
 }
};

// Add this callback to application creation or activity creation where token will
 be used
tokenProvider.onTokenReady(callback);

// Once you have token in token result callback
// if background refresh is enabled you can call getToken() from same tokenprovider
 object
// if background refresh is disabled you can directly call getToken()(blocking call)
 for new token
WAFToken token = tokenProvider.getToken();
```

Ejemplo de Kotlin:

```
import com.amazonaws.waf.mobilesdk.token.WAFConfiguration
import com.amazonaws.waf.mobilesdk.token.WAFTokenProvider
```

```
private lateinit var wafConfiguration: WAFConfiguration
private lateinit var wafTokenProvider: WAFTokenProvider

private val WAF_INTEGRATION_URL = "Web ACL integration URL"
private val WAF_DOMAIN_NAME = "Domain name"

fun initWaf() {
 // Initialize the tokenprovider instance
 val applicationIntegrationURL = URL(WAF_INTEGRATION_URL)
 wafConfiguration =
  WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL)
   .domainName(WAF_DOMAIN_NAME).backgroundRefreshEnabled(true).build()
 wafTokenProvider = WAFTokenProvider(getApplication(), wafConfiguration)

  // getToken from tokenprovider object
  println("WAF: "+ wafTokenProvider.token.value)

  // implement callback for where token will be used
  wafTokenProvider.onTokenReady {
   wafToken, sdkError ->
  run {
   println("WAF Token:" + wafToken.value)
  }
 }
}
```

Permisión de que el SDK proporcione la cookie de token en sus solicitudes HTTP

Si `setTokenCookie` es `TRUE`, el proveedor de tokens incluye la cookie de token para usted en sus solicitudes web en todas las ubicaciones de la ruta especificada en `tokenCookiePath`. De forma predeterminada, `setTokenCookie` es `TRUE` y `tokenCookiePath` es `/`.

Puede limitar el alcance de las solicitudes que incluyen una cookie de token especificando la ruta de la cookie de token, por ejemplo, `/web/login`. Si lo haces, comprueba que tus AWS WAF reglas no inspeccionen los tokens en las solicitudes que envíes a otras rutas. Cuando usa el grupo de reglas de `AWSManagedRulesACFPRuleSet`, configura las rutas de registro y creación de cuentas, y el grupo de reglas comprueba si hay tokens en las solicitudes que se envían a esas rutas. Para obtener más información, consulte Adición del grupo de reglas administradas por ACFP a la nueva ACL web. Igualmente, al usar el grupo de reglas de `AWSManagedRulesATPRuleSet`, configure la ruta de inicio de sesión, y el grupo de reglas comprueba si hay tokens en las solicitudes que se envían a esa

ruta. Para obtener más información, consulte Adición del grupo de reglas administradas por ATP a la nueva ACL web.

iOS

Cuando `setTokenCookie` es `TRUE` así, el proveedor del token almacena el AWS WAF token en un `HTTPCookieStorage.shared` e incluye automáticamente la cookie en las solicitudes al dominio que especificaste`WAFConfiguration`.

```
let request = URLRequest(url: URL(string: domainEndpointUrl)!)
//The token cookie is set automatically as cookie header
let task = URLSession.shared.dataTask(with: request) { data, urlResponse, error  in
}.resume()
```

Android

Cuando `setTokenCookie` es`TRUE`, el proveedor del token almacena el AWS WAF token en una `CookieHandler` instancia que se comparte en toda la aplicación. Cuando el proveedor de tokens incluye automáticamente la cookie en las solicitudes al dominio que especificó en `WAFConfiguration`.

Ejemplo de Java:

```
URL url = new URL("Domain name");
//The token cookie is set automatically as cookie header
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
connection.getResponseCode();
```

Ejemplo de Kotlin:

```
val url = URL("Domain name")
//The token cookie is set automatically as cookie header
val connection = (url.openConnection() as HttpsURLConnection)
connection.responseCode
```

Si ya tiene inicializada la instancia predeterminada `CookieHandler`, el proveedor de tokens la usará para administrar las cookies. De lo contrario, el proveedor del token inicializará una nueva `CookieManager` instancia con el AWS WAF token `CookiePolicy.ACCEPT_ORIGINAL_SERVER` y, a continuación, establecerá esta nueva instancia como la instancia predeterminada en`CookieHandler`.

El siguiente código muestra cómo el SDK inicializa el administrador de cookies y el controlador de cookies cuando no están disponibles en su aplicación.

Ejemplo de Java:

```
CookieManager cookieManager = (CookieManager) CookieHandler.getDefault();
if (cookieManager == null) {
 // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
 cookieManager = new CookieManager();
 CookieHandler.setDefault(cookieManager);
}
```

Ejemplo de Kotlin:

```
var cookieManager = CookieHandler.getDefault() as? CookieManager
if (cookieManager == null) {
 // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
 cookieManager = CookieManager()
 CookieHandler.setDefault(cookieManager)
}
```

Suministro manual de la cookie de token en sus solicitudes HTTP

Si configura `setTokenCookie` en `FALSE`, tendrá que proporcionar la cookie de token manualmente, como encabezado de solicitud HTTP de cookie, en las solicitudes que envíe a su punto de conexión protegido. El siguiente código muestra cómo hacerlo.

iOS

```
var request = URLRequest(url: wafProtectedEndpoint)
request.setValue("aws-waf-token=token from token provider", forHTTPHeaderField:
 "Cookie")
request.httpShouldHandleCookies = true
URLSession.shared.dataTask(with: request) { data, response, error in }
```

Android

Ejemplo de Java:

```
URL url = new URL("Domain name");
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
```

```
String wafTokenCookie = "aws-waf-token=token from token provider";
connection.setRequestProperty("Cookie", wafTokenCookie);
connection.getInputStream();
```

Ejemplo de Kotlin:

```
val url = URL("Domain name")
val connection = (url.openConnection() as HttpsURLConnection)
val wafTokenCookie = "aws-waf-token=token from token provider"
connection.setRequestProperty("Cookie", wafTokenCookie)
connection.inputStream
```

CAPTCHAy Challenge en AWS WAF

Puedes configurar tus AWS WAF reglas para ejecutar CAPTCHA o Challenge tomar medidas contra las solicitudes web que coincidan con los criterios de inspección de tu regla. También puedes programar tus aplicaciones JavaScript cliente para que ejecuten acertijos de CAPTCHA y desafíos del navegador de forma local.

Los acertijos de CAPTCHA y los desafíos silenciosos solo se pueden ejecutar cuando los navegadores acceden a los puntos finales HTTPS. Los clientes del navegador deben ejecutarse en contextos seguros para poder adquirir los tokens.

- CAPTCHA— Requiere que el usuario final resuelva un acertijo de CAPTCHA para demostrar que un ser humano está enviando la solicitud. Los rompecabezas de CAPTCHA están pensados para que los humanos los puedan completar con bastante facilidad y rapidez, mientras que, para las computadoras, sean difíciles de completar con éxito o de forma aleatoria con una tasa de éxito significativa.

  En las reglas de ACL web, el CAPTCHA se suele utilizar cuando una Block acción detendría demasiadas solicitudes legítimas, pero dejar pasar todo el tráfico se traduciría en niveles inaceptablemente altos de solicitudes no deseadas, por ejemplo, procedentes de bots. Para obtener información sobre el comportamiento de las acciones de la regla, consulte. Cómo funcionan las acciones de regla AWS WAFCAPTCHA y Challenge

  También puede programar la implementación de un rompecabezas CAPTCHA en las API de integración de aplicaciones de su cliente. Al hacerlo, puede personalizar el comportamiento y la ubicación del rompecabezas en su aplicación cliente. Para obtener más información, consulte AWS WAF integración de aplicaciones cliente.

- Challenge— Ejecuta un desafío silencioso que requiere que la sesión del cliente verifique que se trata de un navegador y no de un bot. La verificación se ejecuta en segundo plano sin la participación del usuario final. Esta es una buena opción para verificar los clientes de los que se sospecha que no son válidos sin que ello repercuta negativamente en la experiencia del usuario final mediante un rompecabezas de CAPTCHA. Para obtener información sobre el comportamiento de las acciones de la regla, consulteCómo funcionan las acciones de regla AWS WAFCAPTCHA y Challenge.

  La acción de regla Challenge es similar al desafío que representan las API de integración de amenazas inteligentes del cliente, que se describe en AWS WAF integración de aplicaciones cliente.

> **Note**
>
> Se le cobrarán tarifas adicionales cuando utilice la acción de regla CAPTCHA o Challenge en una de sus reglas o como anulación de una acción de regla en un grupo de reglas. Para obtener más información, consulte AWS WAF Precios.

Para obtener descripciones de todas las opciones de acción de la regla, consulteAcción de regla.

Temas

- AWS WAF Rompecabezas CAPTCHA
- Cómo funcionan las acciones de regla AWS WAFCAPTCHA y Challenge
- Prácticas recomendadas para usar las acciones CAPTCHA y Challenge

AWS WAF Rompecabezas CAPTCHA

AWS WAF proporciona una funcionalidad CAPTCHA estándar que desafía a los usuarios a confirmar que son seres humanos. CAPTCHA son las siglas de Completely Automated Public Turing test to tell Computers and Humans Apart (Prueba de Turing Completamente Automática y Pública para Diferenciar Computadoras de Humanos). Los rompecabezas de CAPTCHA están diseñados para verificar que un humano está enviando solicitudes y para evitar actividades como el rastreo de páginas web, el uso de credenciales y el correo no deseado. Los acertijos de CAPTCHA no pueden eliminar todas las solicitudes no deseadas. Se han resuelto muchos acertijos mediante el aprendizaje automático y la inteligencia artificial. En un esfuerzo por evitar el CAPTCHA, algunas organizaciones

complementan las técnicas automatizadas con la intervención humana. A pesar de ello, el CAPTCHA sigue siendo una herramienta útil para evitar el tráfico de bots menos sofisticado y aumentar los recursos necesarios para las operaciones a gran escala.

AWS WAF genera aleatoriamente sus acertijos CAPTCHA y los rota para garantizar que los usuarios se enfrenten a desafíos únicos. AWS WAF añade periódicamente nuevos tipos y estilos de rompecabezas para seguir siendo eficaz frente a las técnicas de automatización. Además de los acertijos, el script AWS WAF CAPTCHA recopila datos sobre el cliente para garantizar que un humano complete la tarea y evitar que se repitan los ataques.

Cada rompecabezas de CAPTCHA incluye un conjunto estándar de controles para que el usuario final pueda solicitar un rompecabezas nuevo, cambiar entre rompecabezas de audio y visuales, acceder a instrucciones adicionales y enviar una solución al rompecabezas. Todos los rompecabezas incluyen soporte para lectores de pantalla, controles de teclado y colores contrastantes.

Los rompecabezas AWS WAF CAPTCHA cumplen con los requisitos de las Pautas de Accesibilidad al Contenido Web (WCAG). Para obtener más información, consulte la Web Content Accessibility Guidelines (WCAG) Overview (descripción general de las directrices de accesibilidad para el contenido web en el sitio web) del World Wide Web Consortium (W3C).

Temas

Soporte para el lenguaje de rompecabezas CAPTCHA

El rompecabezas CAPTCHA comienza con instrucciones escritas en el idioma del navegador del cliente o, si el idioma del navegador no es compatible, en inglés. El rompecabezas ofrece opciones de idiomas alternativos a través de un menú desplegable.

El usuario puede cambiar a las instrucciones de audio seleccionando el icono de los auriculares en la parte inferior de la página. La versión en audio del rompecabezas proporciona instrucciones habladas sobre el texto que el usuario debe escribir en un cuadro de texto, superpuestas por el ruido de fondo.

La siguiente tabla muestra los idiomas que puede seleccionar para las instrucciones escritas de un rompecabezas de CAPTCHA y el soporte de audio para cada selección.

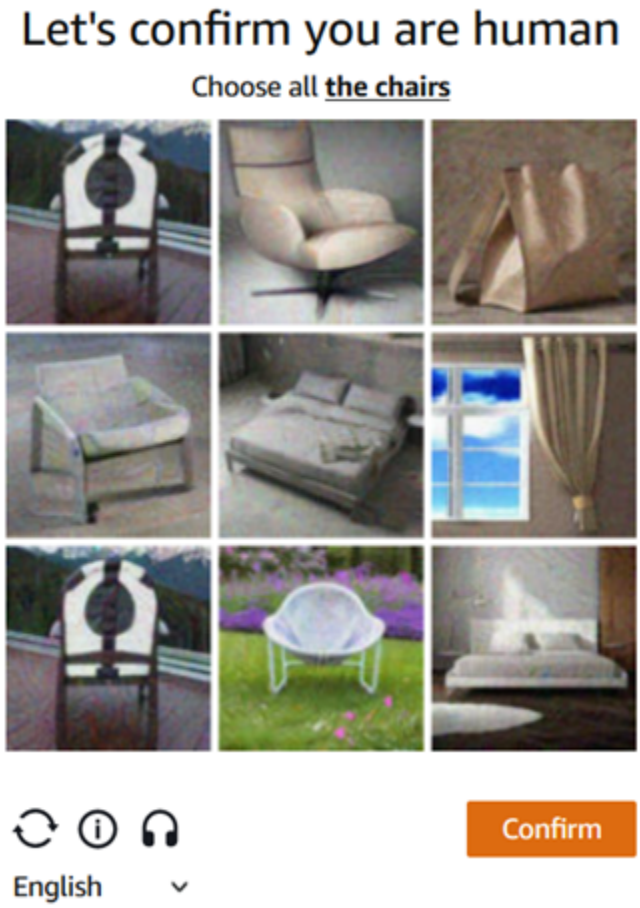
AWS WAF Idiomas compatibles con los rompecabezas CAPTCHA

Soporte para instrucciones escritas	Código local	Soporte de instrucciones de audio
Árabe	Ar-sa	Árabe
Chino simplificado	zh-CN	Audio en inglés
Neerlandés	nl-NL	Neerlandés
Inglés	en-US	Inglés
Francés	fr-FR	Francés
Alemán	de-DE	Alemán
Italiano	it-IT	Italiano
Japonés	ja-JP	Audio en inglés
Portugués de Brasil	pt-BR	Portugués de Brasil
Español	es-ES	Español
Turco	tr-TR	Turco

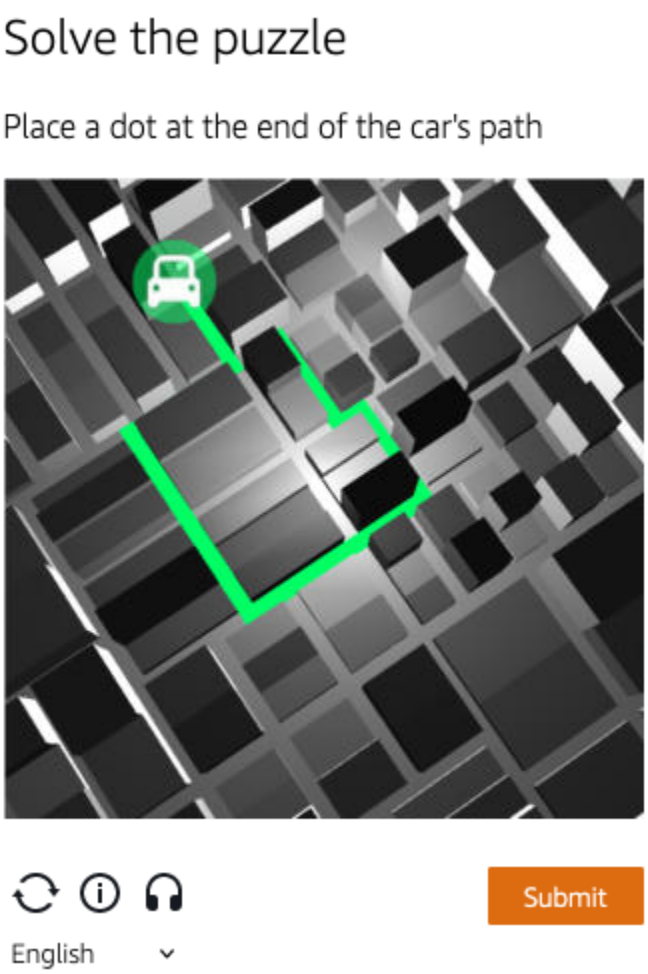
Ejemplos de rompecabezas CAPTCHA

Un típico rompecabezas visual de CAPTCHA requiere interacción para demostrar que el usuario puede comprender e interactuar con una o más imágenes.

La siguiente captura de pantalla muestra un ejemplo de un rompecabezas cuadriculado con imágenes. Este rompecabezas requiere que selecciones todas las imágenes de la cuadrícula que incluyen un tipo específico de objeto.

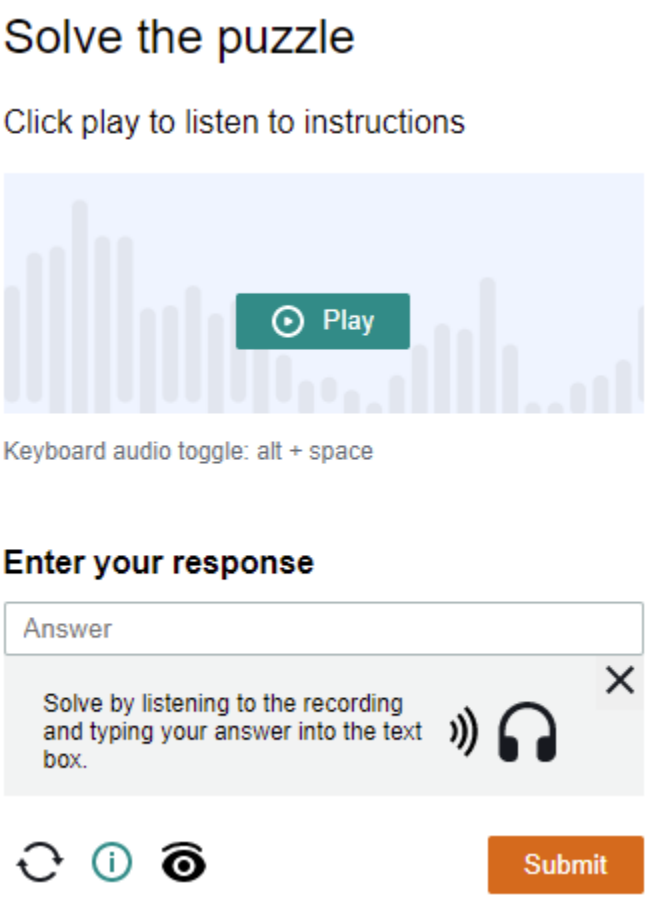


La siguiente captura de pantalla muestra un ejemplo de rompecabezas que requiere que identifiques el punto final de la trayectoria de un automóvil en un dibujo.



Un rompecabezas de audio genera ruido de fondo y se superpone con instrucciones habladas sobre el texto que el usuario debe escribir en un cuadro de texto.

En la siguiente captura de pantalla, se muestra la pantalla para la elección del rompecabezas de audio.



Cómo funcionan las acciones de regla AWS WAFCAPTCHA y Challenge

AWS WAF CAPTCHAy Challenge son acciones de reglas estándar, por lo que son relativamente fáciles de implementar. Para usar cualquiera de ellas, debe crear los criterios de inspección de la regla que identifican las solicitudes que desea inspeccionar y, a continuación, especificar una de las dos acciones de la regla. Para obtener información general sobre las opciones de acciones de las reglas, consulte Acción de regla.

Además de implementar desafíos silenciosos y acertijos CAPTCHA desde el lado del servidor, puede integrar desafíos silenciosos en sus aplicaciones cliente de JavaScript iOS y Android, y puede renderizar rompecabezas CAPTCHA en sus clientes. JavaScript Estas integraciones le permiten ofrecer a sus usuarios finales un mejor rendimiento y una mejor experiencia con los rompecabezas de CAPTCHA, además de reducir los costos asociados al uso de las acciones de regla y los grupos de reglas de mitigación de amenazas inteligentes. Para obtener más información sobre estas opciones, consulte AWS WAF integración de aplicaciones cliente. Para obtener información acerca de los precios, consulte AWS WAF Pricing (Precios de Glue).

Temas

Comportamiento de acción CAPTCHA y Challenge

Cuando una solicitud web coincide con los criterios de inspección de una regla CAPTCHA o una Challenge acción, AWS WAF determina cómo gestionar la solicitud según el estado de su token y la configuración del tiempo de inmunidad. AWS WAF también tiene en cuenta si la solicitud puede gestionar el rompecabezas de CAPTCHA o los intersticiales de los scripts de desafío. Los scripts están diseñados para ser tratados como contenido HTML y solo un cliente que espere contenido HTML puede gestionarlos correctamente.

> **Note**
>
> Se le cobrarán tarifas adicionales cuando utilice la acción de regla CAPTCHA o Challenge en una de sus reglas o como anulación de una acción de regla en un grupo de reglas. Para obtener más información, consulte AWS WAF Precios.

Cómo gestiona la acción la solicitud web

AWS WAF aplica la Challenge acción CAPTCHA o a una solicitud web de la siguiente manera:

- Token válido: lo AWS WAF gestiona de forma similar a una Count acción. AWS WAF aplica todas las etiquetas y personalizaciones de solicitud que haya configurado para la acción de la regla y, a continuación, continúa evaluando la solicitud con las demás reglas de la ACL web.
- Token faltante, no válido o caducado: AWS WAF interrumpe la evaluación de la solicitud mediante ACL web e impide que se dirija a su destino previsto.

  AWS WAF genera una respuesta que envía al cliente, según el tipo de acción de la regla:

  - Challenge: AWS WAF incluye lo que se detalla a continuación en la respuesta:
    - El encabezado `x-amzn-waf-action` con un valor de `challenge`.

> **Note**
>
> Este encabezado no está disponible para JavaScript las aplicaciones que se ejecutan en el navegador del cliente. Para obtener detalles, consulte la siguiente sección.

- El código de estado HTTP `202 Request Accepted`.
- Si la solicitud contiene un `Accept` encabezado con un valor `detext/html`, la respuesta incluye un intersticial de JavaScript página con un script de desafío.

- CAPTCHA— AWS WAF incluye lo siguiente en la respuesta:
  - El encabezado `x-amzn-waf-action` con un valor de `captcha`.

> **Note**
>
> Este encabezado no está disponible para JavaScript las aplicaciones que se ejecutan en el navegador del cliente. Para obtener detalles, consulte la siguiente sección.

  - El código de estado HTTP `405 Method Not Allowed`.
  - Si la solicitud contiene un `Accept` encabezado con un valor `detext/html`, la respuesta incluye un intersticial de JavaScript página con un script CAPTCHA.

Para configurar el momento de vencimiento del token a nivel de reglas o ACL web, consulte Caducidad de la marca de tiempo: tiempos de inmunidad AWS WAF simbólica.

Los encabezados no están disponibles para las JavaScript aplicaciones que se ejecutan en el navegador del cliente

Cuando AWS WAF responde a una solicitud de un cliente con un CAPTCHA o una respuesta a un desafío, no incluye los encabezados de intercambio de recursos entre orígenes (CORS). Los encabezados CORS son un conjunto de encabezados de control de acceso que indican al navegador web del cliente qué dominios, métodos HTTP y encabezados HTTP pueden utilizar las aplicaciones. JavaScript Sin los encabezados CORS, JavaScript las aplicaciones que se ejecutan en el navegador de un cliente no tienen acceso a los encabezados HTTP y, por lo tanto, no pueden leer el `x-amzn-waf-action` encabezado que se proporciona en las respuestas y. CAPTCHA Challenge

Función de los intersticiales de desafío y CAPTCHA

Cuando se ejecuta un desafío intersticial, después de que el cliente responda correctamente, si aún no tiene un token, el intersticial inicializa uno para él. A continuación, actualiza el token con la marca de tiempo de resolución del desafío.

Cuando se ejecuta un intersticial de CAPTCHA, si el cliente aún no tiene un token, el intersticial de CAPTCHA invoca primero el script de desafío para desafiar al navegador e inicializar el token. Luego, el intersticial ejecuta su rompecabezas de CAPTCHA. Cuando el usuario final complete correctamente el rompecabezas, el intersticial actualiza el token con la marca de tiempo de resolución del CAPTCHA.

En cualquier caso, una vez que el cliente responde correctamente y el script actualiza el token, el script vuelve a enviar la solicitud web original utilizando el token actualizado.

Puede configurar la forma AWS WAF en que gestiona los tokens. Para obtener más información, consulte AWS WAF tokens de solicitud web.

Acciones CAPTCHA y Challenge en los registros y las métricas

Las acciones CAPTCHA y Challenge pueden ser de no finalización, como Count, o de finalización, como Block. El resultado depende de si la solicitud tiene un token válido con una marca de tiempo vigente para el tipo de acción.

- Token válido: cuando la acción encuentra un token válido y no bloquea la solicitud, AWS WAF captura las métricas y los registros de la siguiente manera:
  - Incrementa las métricas de `CaptchaRequests` y `RequestsWithValidCaptchaToken` o `ChallengeRequests` y `RequestsWithValidChallengeToken`.
  - Registra la coincidencia como una entrada `nonTerminatingMatchingRules` con una acción CAPTCHA o Challenge. La siguiente lista muestra la sección de un registro para este tipo de coincidencia con la acción CAPTCHA.

```
"nonTerminatingMatchingRules": [
{
  "ruleId": "captcha-rule",
  "action": "CAPTCHA",
  "ruleMatchDetails": [],
  "captchaResponse": {
    "responseCode": 0,
    "solveTimestamp": 1632420429
  }
}
```

```
  ]
```

- Token faltante, no válido o caducado: cuando la acción bloquea la solicitud porque falta un token o no es válido, AWS WAF captura las métricas y los registros de la siguiente manera:
  - Incrementa la métrica para `CaptchaRequests` o `ChallengeRequests`.
  - Registra la coincidencia como una entrada `CaptchaResponse` con código de estado HTTP `405` o como una entrada `ChallengeResponse` con código de estado HTTP `202`. El registro indica si a la solicitud le faltaba el token o si tenía una marca de tiempo caducada. El registro también indica si AWS WAF se envió una página intersticial de CAPTCHA al cliente o si se envió un desafío silencioso al navegador del cliente. La siguiente lista muestra la sección de un registro para este tipo de coincidencia con la acción de CAPTCHA.

```
"terminatingRuleId": "captcha-rule",
"terminatingRuleType": "REGULAR",
"action": "CAPTCHA",
"terminatingRuleMatchDetails": [],
...
"responseCodeSent": 405,
...
"captchaResponse": {
  "responseCode": 405,
  "solveTimestamp": 0,
  "failureReason": "TOKEN_MISSING"
}
```

Para obtener información sobre los registros, consulte AWS WAF . Registro del tráfico de ACL AWS WAF web

Para obtener información sobre AWS WAF las métricas, consulteAWS WAF métricas y dimensiones.

Para obtener información sobre las opciones de acciones de las reglas, consulte Acción de regla.

Prácticas recomendadas para usar las acciones CAPTCHA y Challenge

Siga las instrucciones de esta sección para planificar e implementar el AWS WAF CAPTCHA o el desafío.

Planificación de la implementación del CAPTCHA y el desafío

Determina dónde colocar los rompecabezas de CAPTCHA o los desafíos silenciosos en función del uso de su sitio web, la confidencialidad de los datos que desea proteger y el tipo de solicitudes. Seleccione las solicitudes a las que vaya a aplicar el CAPTCHA para poder presentar los rompecabezas según sea necesario, pero evita presentarlos donde no sean útiles y puedan degradar la experiencia del usuario. Usa esta Challenge acción para ejecutar desafíos silenciosos que tengan un menor impacto en el usuario final y, al mismo tiempo, ayuden a verificar que la solicitud proviene de un navegador JavaScript habilitado.

Los acertijos de CAPTCHA y los desafíos silenciosos solo se pueden ejecutar cuando los navegadores acceden a los puntos finales HTTPS. Los clientes del navegador deben ejecutarse en contextos seguros para poder adquirir los tokens.

Definalización de dónde ejecutar los rompecabezas de CAPTCHA y los desafíos silenciosos para los clientes

Identifique las solicitudes que no desee que se vean afectadas por el CAPTCHA, por ejemplo, las solicitudes de CSS o imágenes. Utilizar CAPTCHA solo cuando sea necesario. Por ejemplo, si planea comprobar el CAPTCHA al iniciar sesión y siempre se redirige al usuario directamente desde el inicio de sesión a otra pantalla, probablemente no sea necesario comprobar el CAPTCHA en la segunda pantalla ya que esto podría perjudicar la experiencia de usuario final.

Configura los tuyos Challenge y CAPTCHA úsalos para que AWS WAF solo envíes acertijos CAPTCHA y desafíos silenciosos en respuesta a las `GET` `text/html` solicitudes. No puede ejecutar el rompecabezas ni el desafío en respuesta a solicitudes `POST`, solicitudes `OPTIONS` de verificación previa del uso compartido de recursos entre orígenes (CORS) o cualquier otro tipo de solicitud que no sea `GET`. El comportamiento del navegador para otros tipos de solicitudes puede variar y es posible que no pueda gestionar los intersticiales correctamente.

Es posible que un cliente acepte HTML y, aun así, no pueda gestionar el CAPTCHA ni cuestionar los intersticiales. Por ejemplo, un widget de una página web con un iFrame pequeño puede aceptar HTML, pero no mostrar un CAPTCHA ni procesarlo. Evite incluir las acciones de regla para este tipo de solicitudes, igual que para las solicitudes que no aceptan HTML.

Uso de CAPTCHA o Challenge para verificar la adquisición previa del token

Puede usar las acciones de la regla únicamente para verificar la existencia de un token válido en ubicaciones donde los usuarios legítimos siempre deberían tener uno. En estas situaciones, no importa si la solicitud puede gestionar los intersticiales.

Por ejemplo, si implementa la API CAPTCHA de la aplicación JavaScript cliente y ejecuta el rompecabezas de CAPTCHA en el cliente inmediatamente antes de enviar la primera solicitud a su terminal protegido, la primera solicitud siempre debe incluir un token que sea válido tanto para la impugnación como para el CAPTCHA. Para obtener información sobre la integración de aplicaciones cliente, consulte JavaScript . AWS WAF JavaScript integraciones

En este caso, en su ACL web, puede agregar una regla que coincida con esta primera llamada y configurarla con la acción de regla Challenge o CAPTCHA. Cuando la regla coincida entre un usuario final legítimo y un navegador, la acción buscará un token válido y, por lo tanto, no bloqueará la solicitud ni enviará un desafío o un rompecabezas de CAPTCHA como respuesta. Para obtener más información sobre cómo funcionan las etiquetas, consulte Comportamiento de acción CAPTCHA y Challenge.

Protección de datos confidenciales que no sean HTML con CAPTCHA y Challenge

Puede usar el CAPTCHA y las protecciones Challenge para datos confidenciales que no sean HTML, como las API, con el siguiente enfoque.

1. Identifique las solicitudes que aceptan respuestas HTML y que se ejecutan muy cerca de las solicitudes de sus datos confidenciales que no son HTML.
2. Escriba reglas CAPTCHA o Challenge que coincidan con las solicitudes HTML y con las solicitudes de sus datos confidenciales.
3. Ajuste su configuración del tiempo de inmunidad de CAPTCHA y Challenge para que, en las interacciones normales de los usuarios, los tokens que los clientes obtienen de las solicitudes de HTML estén disponibles y no hayan caducado en sus solicitudes de datos confidenciales. Para obtener información sobre el ajuste, consulte Caducidad de la marca de tiempo: tiempos de inmunidad AWS WAF simbólica.

Si una solicitud de datos confidenciales coincide con una regla CAPTCHA o Challenge, no se bloqueará si el cliente aún tiene un token válido del rompecabezas o desafío anterior. Si el token no está disponible o la marca de tiempo ha caducado, la solicitud de acceso a sus datos confidenciales fallará. Para obtener más información sobre cómo funcionan las etiquetas, consulte Comportamiento de acción CAPTCHA y Challenge.

Uso de CAPTCHA y Challenge para ajustar las reglas existentes

Revise sus reglas actuales para ver si quiere modificarlas o agregarlas. A continuación, se presentan algunos escenarios comunes a considerar.

- Si tiene una regla basada en tasas que bloquea el tráfico, pero mantiene el límite de tasa relativamente alto para evitar bloquear a los usuarios legítimos, considere la posibilidad de agregar una segunda regla basada tasas después de la regla de bloqueo. Asigne a la segunda regla un límite inferior al de la regla de bloqueo y establezca la acción de regla en CAPTCHA o Challenge. La regla de bloqueo seguirá bloqueando las solicitudes que lleguen a un ritmo demasiado alto y la nueva regla bloqueará la mayor parte del tráfico automatizado a un ritmo aún menor. Para obtener información acerca de las reglas basadas en tasas, consulte Instrucción de regla basada en frecuencia.
- Si tiene un grupo de reglas administrado que bloquea las solicitudes, puede cambiar el comportamiento de algunas o todas las reglas de Block a CAPTCHA o Challenge. Para ello, en la configuración del grupo de reglas administrado, anule la configuración de la acción de regla. Para obtener información sobre la anulaciones de las acciones de las reglas, consulte La acción de la regla del grupo de reglas anula.

Comprobación de las implementaciones del CAPTCHA y el desafío antes de implantarlas

En cuanto a todas las nuevas funciones, siga las instrucciones que se indican en the section called “Pruebas y ajustes de sus protecciones”.

Durante las pruebas, revise los requisitos de caducidad de las marcas de tiempo de los tokens y establezca las configuraciones de tiempo de inmunidad de las reglas y la ACL web para lograr un buen equilibrio entre el control del acceso a su sitio web y el suministro de una buena experiencia a sus clientes. Para obtener más información, consulte Caducidad de la marca de tiempo: tiempos de inmunidad AWS WAF simbólica.

Registro del tráfico de ACL AWS WAF web

Puede habilitar el registro para obtener información detallada sobre el tráfico que analiza su ACL web. La información registrada incluye la hora en que se AWS WAF recibió una solicitud web de su AWS recurso, información detallada sobre la solicitud y detalles sobre las reglas con las que se ajustó la solicitud. Puede enviar registros de ACL web a un grupo de CloudWatch registros de Amazon Logs, a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de entrega de Amazon Data Firehose.

Otras opciones de recopilación y análisis de datos

Además del registro, puede habilitar las siguientes opciones para la recopilación y el análisis de datos:

- Amazon Security Lake: puede configurar Security Lake para recopilar datos de ACL web. Security Lake recopila datos de registros y eventos de diversas fuentes para su normalización, análisis y administración. Para obtener información sobre esta opción, consulte ¿Qué es Amazon Security Lake? y Recopilación de datos de AWS los servicios de la guía del usuario de Amazon Security Lake.

  AWS WAF no le cobra por usar esta opción. Para obtener información sobre precios, consulte los precios de Security Lake y Cómo se determinan los precios de Security Lake en la guía del usuario de Amazon Security Lake.
- Solicitar muestreo: puede configurar su ACL web para que muestree las solicitudes web que evalúa, a fin de hacerse una idea del tipo de tráfico que recibe su aplicación. Para obtener más información acerca de esta opción, consulte Visualizar una muestra de solicitudes web.

> **Note**
>
> La configuración del registro de la ACL web solo afecta a los AWS WAF registros. En particular, la configuración de los campos redactados para el registro no afecta al muestreo solicitado ni a la recopilación de datos de Security Lake. La recopilación de datos de Security Lake se configura completamente a través del servicio Security Lake. La única forma de excluir campos de las solicitudes muestreadas es deshabilitar el muestreo para la ACL web.

Temas

Precios para registrar la información de tráfico de la ACL web

Se le cobrará por registrar la información del tráfico de la ACL web de acuerdo con los costos asociados a cada tipo de destino de registro. Estos cargos se suman a los cargos de uso de AWS WAF. Los costos pueden variar en función de factores como el tipo de destino que elija y la cantidad de datos que registre.

A continuación, se proporcionan enlaces a la información de precios de cada tipo de destino de registro:

- CloudWatch Registros: los cargos corresponden a la entrega de troncos vendidos. Consulta los precios CloudWatch de Amazon Logs. En el nivel de pago, selecciona la pestaña Logs y, a continuación, en Vended Logs, consulta la información sobre la entrega a CloudWatch Logs.
- Depósitos de Amazon S3: los cargos de Amazon S3 son los cargos combinados por la entrega de CloudWatch registros vendidos a los cubos de Amazon S3 y por el uso de Amazon S3.
  - Para Amazon S3, consulte Precios de Amazon S3.
  - Para obtener CloudWatch información sobre la entrega de registros vendidos a Amazon S3, consulte los precios de Amazon CloudWatch Logs. En Nivel de pago, seleccione la pestaña Registros y, a continuación, en Registros vendidos, consulte la información sobre el Envío a S3.
- Firehose: consulta los precios de Amazon Data Firehose.

Para obtener información sobre AWS WAF los precios, consulte AWS WAF Precios.

AWS WAF destinos de registro

En esta sección se describen los destinos de registro que puede elegir para los registros de AWS WAF . Cada sección proporciona instrucciones a fin de configurar el registro para el tipo de destino que incluye información sobre cualquier comportamiento específico del tipo de destino. Después de configurar el destino de registro, puede agregar especificaciones a la configuración de registro de la ACL web para iniciar el registro en él.

Temas

- Grupo de CloudWatch registros de Amazon Logs
- Depósito de Amazon Simple Storage Service
- Transmisión de entrega de Amazon Data Firehose

Grupo de CloudWatch registros de Amazon Logs

En este tema se proporciona información para enviar los registros de tráfico de ACL web a un grupo de CloudWatch registros.

> **Note**
>
> Se le cobrará por el registro además de los cargos por su uso de AWS WAF. Para obtener más información, consulte Precios para registrar la información de tráfico de la ACL web.

Para enviar registros a Amazon CloudWatch Logs, debe crear un grupo de CloudWatch registros de registros. Cuando habilita el inicio de sesión AWS WAF, proporciona el ARN del grupo de registros. Después de habilitar el registro para su ACL web, AWS WAF envía los registros al grupo de CloudWatch registros en flujos de registros.

Al utilizar CloudWatch los registros, puede explorar los registros de su ACL web en la AWS WAF consola. En su página web de ACL, seleccione la pestaña Registro de información. Esta opción se suma a la información de registro que se proporciona para CloudWatch los registros a través de la CloudWatch consola.

Configure el grupo de registros para los registros de la ACL AWS WAF web en la misma región que la ACL web y con la misma cuenta que utilizó para administrar la ACL web. Para obtener información sobre la configuración de un grupo de CloudWatch registros, consulte Trabajar con grupos de registros y flujos de registros.

Cuotas para CloudWatch los grupos de registros

CloudWatch Logs tiene una cuota máxima de rendimiento predeterminada, que se comparte entre todos los grupos de registros de una región, y que puede solicitar que se aumente. Si tus requisitos de registro son demasiado altos para la configuración de rendimiento actual, verás las métricas de limitación de tu cuenta. `PutLogEvents` Para ver el límite en la consola de Service Quotas y solicitar un aumento, consulta la PutLogEvents cuota de CloudWatch Logs.

Denominación de grupos de registro

Los nombres de sus grupos de registro deben empezar `aws-waf-logs-` por y terminar con el sufijo que desee, por ejemplo, `aws-waf-logs-testLogGroup2`.

El formato del ARN resultante es el siguiente:

```
arn:aws:logs:Region:account-id:log-group:aws-waf-logs-log-group-suffix
```

Los flujos de registros tienen un formato similar al siguiente:

```
Region_web-acl-name_log-stream-number
```

A continuación se muestra un ejemplo de flujo de registro para la ACL web `TestWebACL` en la región `us-east-1`.

```
us-east-1_TestWebACL_0
```

Permisos necesarios para publicar CloudWatch registros en Logs

La configuración del registro de tráfico de ACL web para un grupo de CloudWatch registros requiere la configuración de permisos que se describe en esta sección. Los permisos se configuran automáticamente cuando utiliza una de las políticas gestionadas de acceso AWS WAF completo, `AWSWAFConsoleFullAccess` o bien`AWSWAFFullAccess`. Si desea administrar un acceso más detallado a sus registros y AWS WAF recursos, puede configurar los permisos usted mismo. Para obtener información sobre la administración de permisos, consulte Administración del acceso a AWS los recursos en la Guía del usuario de IAM. Para obtener información sobre las políticas administradas de AWS WAF , consulte AWS políticas gestionadas para AWS WAF.

Estos permisos le permiten cambiar la configuración de registro de la ACL web, configurar la entrega de CloudWatch registros para los registros y recuperar información sobre su grupo de registros. Estos permisos deben estar asociados al usuario que utilice para administrar AWS WAF.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[

            "wafv2:PutLoggingConfiguration",
            "wafv2:DeleteLoggingConfiguration"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow",
         "Sid":"LoggingConfigurationAPI"
      }
      {
         "Sid":"WebACLLoggingCWL",
         "Action":[
```

```
            "logs:CreateLogDelivery",
            "logs:DeleteLogDelivery",
            "logs:PutResourcePolicy",
            "logs:DescribeResourcePolicies",
            "logs:DescribeLogGroups"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow"
      }
   ]
}
```

Cuando se permiten acciones en todos AWS los recursos, se indica en la política con una `"Resource"` configuración de`"*"`. Esto significa que las acciones están permitidas en todos los AWS recursos compatibles con cada acción. Por ejemplo, la acción `wafv2:PutLoggingConfiguration` solo se admite para registrar los recursos de configuración `wafv2`.

Depósito de Amazon Simple Storage Service

En este tema se proporciona información para enviar los registros de tráfico de ACL web a un bucket de Amazon S3.

> **Note**
>
> Se le cobrará por el registro además de los cargos por su uso de AWS WAF. Para obtener más información, consulte Precios para registrar la información de tráfico de la ACL web.

Para enviar los registros de tráfico de la ACL web a Amazon S3, debe configurar un bucket de Amazon S3 desde la misma cuenta que utiliza para gestionar la ACL web y asignarle un nombre al depósito que empiece por `aws-waf-logs-`. Cuando habilitas el inicio de sesión AWS WAF, indicas el nombre del bucket. Para obtener información acerca de la creación de un bucket de registro, consulte Crear un bucket en la Guía del usuario de Amazon Simple Storage Service.

Puede acceder a sus registros de Amazon S3 y analizarlos mediante el servicio de consultas interactivas de Amazon Athena. Athena facilita el análisis de datos directamente en Amazon S3 con SQL estándar. Con unas cuantas acciones AWS Management Console, puede dirigir a Athena a los

datos almacenados en Amazon S3 y empezar a utilizar rápidamente el SQL estándar para ejecutar consultas ad hoc y obtener resultados. Para obtener más información, consulte Consultas de AWS WAF registros en la guía del usuario de Amazon Athena.

> **Note**
>
> AWS WAF admite el cifrado con buckets de Amazon S3 para el tipo de clave clave Amazon S3 (SSE-S3) y para AWS Key Management Service (SSE-KMS). AWS KMS keys AWS WAF no admite el cifrado de AWS Key Management Service las claves administradas por. AWS

Sus ACL web publican sus archivos de registro en el bucket de Amazon S3 en intervalos de cinco minutos. Cada archivo de registro contiene registros de flujo del tráfico IP registrado en los cinco minutos anteriores.

El tamaño de archivo máximo de un archivo log es de 75 MB. Si el archivo de registro alcanza el límite de tamaño de archivo en el periodo de cinco minutos, el registro deja de agregar registros a este archivo, lo publica en el bucket de Amazon S3 y después crea un nuevo archivo de registro.

Los archivos log están comprimidos. Si abre los archivos de registro con la consola de Amazon S3, se descomprimen y se muestran las entradas de registro. Si descarga los archivos de registro, debe descomprimirlos para verlos.

Un único archivo de registro contiene entradas intercaladas con varios registros. Para ver todos los archivos de registro de una ACL web, busque las entradas agregadas por el nombre de la ACL web, la región y el ID de su cuenta.

Requisitos de nomenclatura y sintaxis

Los nombres de los AWS WAF buckets para el registro deben empezar `aws-waf-logs-` y terminar con el sufijo que desee. Por ejemplo, `aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX`.

Ubicación del bucket

Las ubicaciones de los buckets utilizan la siguiente sintaxis:

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/
```

ARN de bucket

El formato del bucket tiene el siguiente formato de Nombre de recurso de Amazon (ARN):

```
arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX
```

Ubicaciones de los buckets con prefijos

Si usa prefijos en el nombre de las claves de sus objetos para organizar los datos que almacena en sus depósitos, puede incluir sus prefijos en los nombres de los buckets de registro.

> **Note**
>
> Esta opción no está disponible en la consola. Utilice las AWS WAF API, la CLI o AWS CloudFormation.

Para obtener información acerca del uso de prefijos en Amazon S3consulte Organizar objetos usando prefijos en la Guía para usuarios de Amazon Simple Storage Service.

Las ubicaciones de los buckets con prefijos utilizan la siguiente sintaxis:

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/DOC-EXAMPLE-KEY-NAME-PREFIX/
```

Carpetas de buckets y nombres de archivos

Dentro de sus grupos y siguiendo los prefijos que proporcione, sus AWS WAF registros se escriben en una estructura de carpetas determinada por su ID de cuenta, la región, el nombre de la ACL web y la fecha y la hora.

```
AWSLogs/account-id/WAFLogs/Region/web-acl-name/YYYY/MM/dd/HH/mm
```

Dentro de las carpetas, los nombres de los archivos de registro siguen un formato similar:

```
account-id_waflogs_Region_web-acl-name_timestamp_hash.log.gz
```

Las especificaciones de tiempo utilizadas en la estructura de carpetas y en el nombre del archivo de registro se ajustan a la especificación del formato de marca de tiempo `YYYYMMddTHHmmZ`.

A continuación, se muestra un archivo de registro de ejemplo en un bucket de Amazon S3 para un bucket llamado `DOC-EXAMPLE-BUCKET`. El Cuenta de AWS es. `11111111111` La ACL web es `TEST-WEBACL` y la región es `us-east-1`.

```
s3://DOC-EXAMPLE-BUCKET/AWSLogs/11111111111/WAFLogs/us-east-1/
TEST-WEBACL/2021/10/28/19/50/11111111111_waflogs_us-east-1_TEST-
WEBACL_20211028T1950Z_e0ca43b5.log.gz
```

> **Note**
>
> Los nombres de los cubos para el AWS WAF registro deben empezar `aws-waf-logs-` y terminar con cualquier sufijo que desee.

Permisos necesarios para publicar registros en Amazon S3

La configuración del registro de tráfico de ACL web para un bucket de Amazon S3 requiere la siguientes configuración de permisos. Configure estos permisos automáticamente cuando utiliza una de las políticas administradas de acceso completo de AWS WAF , `AWSWAFConsoleFullAccess` o `AWSWAFFullAccess`. Si desea administrar un acceso más detallado a sus registros y AWS WAF recursos, puede configurar estos permisos usted mismo. Para obtener más información sobre los permisos de administración, consulte Administración de accesos para recursos de AWS en la Guía del usuario de IAM. Para obtener información sobre las políticas AWS WAF administradas, consulte. AWS políticas gestionadas para AWS WAF

Los siguientes permisos le permiten cambiar la configuración de registro de la ACL web y configurar el envío de registros a su bucket de Amazon S3. Estos permisos deben estar asociados al usuario que utilice para administrar AWS WAF.

> **Note**
>
> Al configurar los permisos que se indican a continuación, es posible que veas errores en tus AWS CloudTrail registros que indiquen que se ha denegado el acceso, pero los permisos de AWS WAF registro son correctos.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "wafv2:PutLoggingConfiguration",
            "wafv2:DeleteLoggingConfiguration"
```

```
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow",
         "Sid":"LoggingConfigurationAPI"
      },
    {

       "Sid":"WebACLLogDelivery",

       "Action":[

          "logs:CreateLogDelivery",

          "logs:DeleteLogDelivery"

       ],

       "Resource": "*",

       "Effect":"Allow"

    },
      {
         "Sid":"WebACLLoggingS3",
         "Action":[
            "s3:PutBucketPolicy",
            "s3:GetBucketPolicy"
         ],
         "Resource": [
                "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET"
         ],
         "Effect":"Allow"
      }
   ]
}
```

Cuando se permiten acciones en todos AWS los recursos, se indica en la política con una `"Resource"` configuración de`"*"`. Esto significa que las acciones están permitidas en todos los AWS recursos compatibles con cada acción. Por ejemplo, la acción `wafv2:PutLoggingConfiguration` solo se admite para registrar los recursos de configuración `wafv2`.

De forma predeterminada, los buckets de Amazon S3 y los objetos que contienen son privados. Solo el propietario del bucket puede tener acceso al bucket y a los objetos almacenados en él. Sin embargo, el propietario del bucket puede conceder permisos de acceso a otros recursos y usuarios escribiendo una política de acceso.

Si el usuario que va a crear el registro es el propietario del bucket, se asocia automáticamente la siguiente política al bucket para conceder al registro permiso para publicar registros en el mismo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/AWSLogs/account-id/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": ["account-id"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": ["account-id"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
```

```
        }
      }
    }
  ]
}
```

> **Note**
>
> Los nombres de los cubos para el AWS WAF registro deben empezar `aws-waf-logs-` y terminar con el sufijo que desee.

Si el usuario que va a crear el registro no es el propietario del bucket, o no tiene los permisos `GetBucketPolicy` y `PutBucketPolicy` para el bucket, se produce un error al crear el registro. En este caso, el propietario del bucket debe agregar manualmente la política anterior al bucket y especificar el ID de la cuenta de Cuenta de AWS del creador del registro. Para obtener más información, consulte How Do I Add an S3 Bucket Policy? (¿Cómo agrego una política de bucket de S3?) en la Guía del usuario de Amazon Simple Storage Service. Si el bucket recibe registros de varias cuentas, agregue un entrada del elemento `Resource` a la instrucción `AWSLogDeliveryWrite` de la política para cada cuenta.

Por ejemplo, la siguiente política de compartimentos Cuenta de AWS `111122223333` permite publicar registros en un depósito denominado`aws-waf-logs-`*`DOC-EXAMPLE-BUCKET`*:

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryWrite20150319",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
                "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/
AWSLogs/111122223333/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": ["111122223333"]
```

```
                },
                "ArnLike": {
                    "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
            "Condition": {
                "StringEquals": {
                "aws:SourceAccount": ["111122223333"]
                },
                "ArnLike": {
                "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
                }
            }
        }
    ]
}
```

Permisos para usar AWS Key Management Service con una clave KMS

Si el destino del registro usa el cifrado del lado del servidor con claves almacenadas en AWS Key Management Service (SSE-KMS) y usted usa una clave administrada por el cliente (clave KMS), debe dar AWS WAF permiso para usar su clave KMS. Para ello, añada una política de claves a la clave KMS del destino que elija. Esto permite que el registro de AWS WAF escriba los archivos de registro en el destino.

Añada la siguiente política clave a su clave de KMS AWS WAF para poder iniciar sesión en su bucket de Amazon S3.

```
{
    "Sid": "Allow AWS WAF to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
```

```
            ]
        },
        "Action": "kms:GenerateDataKey*",
        "Resource": "*"
}
```

Permisos requeridos para acceder a los archivos de registro de Amazon S3

Amazon S3 utiliza listas de control de acceso (ACL) para administrar el acceso a los archivos de registro creados por un registro de AWS WAF . De forma predeterminada, el propietario del bucket tiene los permisos `FULL_CONTROL` en cada archivo log. El propietario de la entrega de logs, si es diferente del propietario del bucket, no tiene permisos. La cuenta de entrega de registros tiene los permisos `READ` y `WRITE`. Para obtener más información, consulte Access Control List (ACL) Overview (Información general de la Lista de control de acceso [ACL]) en la Guía del usuario de Amazon Simple Storage Service.

Transmisión de entrega de Amazon Data Firehose

En esta sección se proporciona información para enviar tus registros de tráfico de ACL web a una transmisión de entrega de Amazon Data Firehose.

> **Note**
>
> Se le cobrará por el registro además de los cargos por su uso de AWS WAF. Para obtener más información, consulte Precios para registrar la información de tráfico de la ACL web.

Para enviar registros a Amazon Data Firehose, debe enviar los registros desde su ACL web a una transmisión de entrega de Amazon Data Firehose que configure en Firehose. Después de habilitar el registro, AWS WAF entrega los registros a su destino de almacenamiento a través del punto de conexión HTTPS de Firehose.

Un AWS WAF registro equivale a un registro de Firehose. Si normalmente recibes 10 000 solicitudes por segundo y habilitas los registros completos, deberías tener una configuración de 10 000 registros por segundo en Firehose. Si no configuras Firehose correctamente, no AWS WAF registrará todos los registros. Para obtener más información, consulte Cuotas de Amazon Kinesis Data Firehose.

Para obtener información sobre cómo crear una transmisión de entrega de Amazon Data Firehose y revisar los registros almacenados, consulta ¿Qué es Amazon Data Firehose?

Para obtener información sobre cómo crear tu flujo de entrega, consulta Cómo crear un flujo de entrega de Amazon Data Firehose.

Configuración de una transmisión de entrega de Amazon Data Firehose para su ACL web

Configure una transmisión de entrega de Amazon Data Firehose para su ACL web de la siguiente manera.

- Créelo con la misma cuenta que utiliza para administrar la ACL web.
- Créelo en la misma región que la ACL web. Si está capturando troncos para Amazon CloudFront, cree la manguera de incendios en la región EE.UU. Este (Norte de Virginia),`us-east-1`.
- Asigne a Data Firehose un nombre que comience con el prefijo `aws-waf-logs-`. Por ejemplo, `aws-waf-logs-us-east-2-analytics`.
- Configúrela para la colocación directa, lo que permite a las aplicaciones acceder directamente al flujo de envío. En la consola Amazon Data Firehose, para configurar la fuente de la transmisión de entrega, elija Direct PUT u otras fuentes. A través de la API, defina la propiedad `DeliveryStreamType` de flujo de envío en `DirectPut`.

> **Note**
>
> No utilice `Kinesis stream` como origen.

Permisos necesarios para publicar registros en una transmisión de entrega de Amazon Data Firehose

Para conocer los permisos necesarios para la configuración de Kinesis Data Firehose, consulte Controlling Access with Amazon Kinesis Data Firehose.

Debe tener los siguientes permisos para habilitar correctamente el registro de ACL web con una transmisión de entrega de Amazon Data Firehose.

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

Para obtener información acerca de los roles vinculados a servicios y el permiso `iam:CreateServiceLinkedRole`, consulte Uso de roles vinculados a servicios para AWS WAF.

Configuración de registro de ACL web

Puede habilitar y desactivar el registro de una ACL web en cualquier momento.

> **Note**
>
> Se le cobrará por el registro además de los cargos por su uso de AWS WAF. Para obtener más información, consulte Precios para registrar la información de tráfico de la ACL web.

Si no puede encontrar una entrada de registro en sus registros

En raras ocasiones, es posible que la entrega de AWS WAF registros caiga por debajo del 100% y que los registros se entreguen haciendo todo lo posible. La AWS WAF arquitectura prioriza la seguridad de las aplicaciones por encima de todas las demás consideraciones. En algunas situaciones, como cuando los flujos de registro sufren una limitación del tráfico, puede haber una pérdida de registros. Esto no debería afectar a muchos registros. Si observa que faltan varias entradas de registro, póngase en contacto con el Centro de AWS Support.

En la configuración de registro de su ACL web, puede personalizar lo que se AWS WAF envía a los registros.

- Redacción de campos: puede redactar los siguientes campos de los registros para las reglas que utilizan la configuración de coincidencia correspondiente: ruta de URI, cadena de consulta, encabezado único y método HTTP. Los campos redactados aparecen como `REDACTED` en los registros. Por ejemplo, si redacta el campo de cadena de consulta, en los registros, aparecerá como `REDACTED` para todas las reglas que utilizan la configuración del componente de coincidencia de cadena de consulta. La redacción solo se aplica al componente de solicitud que especifique para que coincida en la regla, por lo que la redacción del componente de encabezado único no se aplica a las reglas que coinciden con los encabezados. Para obtener una lista de los campos de registro, consulte Campos de registro.

  > **Note**
  >
  > Esta configuración no afecta al muestreo de las solicitudes. En el caso de las solicitudes de muestreo, la única forma de excluir los campos es inhabilitando el muestreo para la ACL web.

- Filtrado de registros: puede agregar filtros para especificar qué solicitudes web se conservan en los registros y cuáles se eliminan. Se filtra según la configuración que AWS WAF se aplica durante la evaluación de la solicitud web. Puede añadir filtros según las siguientes configuraciones:
  - Etiqueta completa: las etiquetas completas tienen un prefijo, espacios de nombres opcionales y un nombre de etiqueta. El prefijo identifica el grupo de reglas o el contexto de ACL web de la regla que agregó la etiqueta. Para obtener información acerca de las etiquetas, consulte AWS WAF etiquetas en las solicitudes web.
  - Acción de regla: puede filtrar por cualquier configuración de acción de regla normal y también por la opción de anulación `EXCLUDED_AS_COUNT` heredada para las reglas de los grupos de reglas. Para obtener información sobre la configuración de las acciones de las reglas, consulte Acción de regla. Para obtener información sobre las anulaciones de acciones de regla actuales y heredadas para las reglas de grupos de reglas, consulte Opciones de anulación de acciones para grupos de reglas.
    - Los filtros de acción de regla normales se aplican a las acciones que se configuran en las reglas y también a las acciones que se configuran mediante la opción actual para anular una acción de regla de un grupo de reglas.
    - El filtro de registro `EXCLUDED_AS_COUNT` se superpone con el filtro de registro de acciones `Count`. `EXCLUDED_AS_COUNT` filtra las opciones actuales y heredadas para anular la acción de una regla de un grupo de reglas a Count.

Habilitar el registro para una ACL web

Para habilitar el registro de una ACL web, debe haber configurado ya un destino de registro. Para obtener información sobre las opciones de destino y los requisitos de cada una de ellas, consulte AWS WAF destinos de registro.

Para habilitar el registro para una ACL web

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, seleccione Web ACLs (ACL web).
3. Elija el nombre de la ACL web para la que desea habilitar el registro. La consola le lleva a la descripción de la ACL web, donde puede editarla.
4. En la pestaña de Registro, elija Habilitar el registro.

5. Elija el tipo de destino del registro y, a continuación, elija el destino del registro que haya configurado. Debe elegir un destino de registro cuyo nombre comience con `aws-waf-logs-`.
6. (Opcional) Si no quiere que se incluyan algunos campos en los registros, redáctelos. Elija el campo que se va a redactar y, a continuación, elija Add (Añadir). Repita según sea necesario para redactar campos adicionales.

   > **Note**
   >
   > Esta configuración no afecta a las solicitudes de muestreo. En el caso de las solicitudes de muestreo, la única forma de excluir los campos es inhabilitando el muestreo para la ACL web.

7. (Opcional) Si no desea enviar todas las solicitudes a los registros, agregue sus criterios de filtrado y su comportamiento. En Filtrar registros, para cada filtro que desee aplicar, elija Agregar filtro y, a continuación, elija sus criterios de filtrado y especifique si desea conservar o eliminar las solicitudes que coincidan con los criterios. Cuando termine de añadir filtros, si es necesario, modifique el comportamiento de registro predeterminado.
8. Elija Enable logging (Habilitar el registro).

   > **Note**
   >
   > Cuando habilite correctamente el registro, AWS WAF se creará un rol vinculado al servicio con los permisos necesarios para escribir los registros en el destino del registro. Para obtener más información, consulte Uso de roles vinculados a servicios para AWS WAF.

Campos de registro

En la siguiente lista se describen los posibles campos del registro.

acción

La acción de finalización que AWS WAF se aplicó a la solicitud. Esto indica permitir, bloquear, CAPTCHA o desafío. Las acciones CAPTCHA y Challenge son de finalización cuando la solicitud web no contiene un token válido.

args

La cadena de consulta.

captchaResponse

El estado de la acción de CAPTCHA de la solicitud, que se rellena cuando se aplica una CAPTCHA acción a la solicitud. Este campo se rellena para cualquier CAPTCHA acción, ya sea finalizada o no. Si en una solicitud se ha aplicado la CAPTCHA acción varias veces, este campo se rellena desde la última vez que se aplicó la acción.

La acción CAPTCHA finaliza la inspección de la solicitud web cuando la solicitud no incluye un token o si el token no es válido o ha vencido. Si la CAPTCHA acción está finalizando, este campo incluye un código de respuesta y el motivo del error. Si la acción no termina, este campo incluye una marca de tiempo de resolución. Para diferenciar entre una acción que termina y una que no termina, puedes filtrar en este campo para ver un atributo que no esté vacío. `failureReason`

challengeResponse

El estado de la acción de impugnación de la solicitud, que se rellena cuando se aplica una Challenge acción a la solicitud. Este campo se rellena para cualquier Challenge acción, ya sea finalizada o no. Si en una solicitud se ha aplicado la Challenge acción varias veces, este campo se rellena desde la última vez que se aplicó la acción.

La acción Challenge finaliza la inspección de la solicitud web cuando la solicitud no incluye un token o si el token no es válido o ha vencido. Si la Challenge acción está finalizando, este campo incluye un código de respuesta y el motivo del error. Si la acción no termina, este campo incluye una marca de tiempo de resolución. Para diferenciar entre una acción que termina y una que no termina, puedes filtrar en este campo para ver un atributo que no esté vacío. `failureReason`

clientIp

La dirección IP del cliente que envía la solicitud.

country

El país de origen de la solicitud. Si AWS WAF no puede determinar el país de origen, establece este campo en. -

excludedRules

Se usa solo para reglas del grupo de reglas. La lista de reglas del grupo de reglas que ha excluido. La acción para estas reglas se establece en Count.

Si anula una regla para contabilizarla mediante la opción de acción de anular regla, las coincidencias no se muestran aquí. Se muestran como parejas de acción `action` y `overriddenAction`.

exclusionType

Un tipo que indica que la regla excluida tiene la acción Count.

ruleId

El ID de la regla del grupo de reglas que se ha excluido.

formatVersion

La versión de formato para el registro.

headers

La lista de encabezados.

httpMethod

El método HTTP en la solicitud.

httpRequest

Los metadatos sobre la solicitud.

httpSourceId

El identificador del recurso asociado:

- En el caso de una CloudFront distribución de Amazon, el ID es el que *`distribution-id`* aparece en la sintaxis del ARN:

  `arn:`*`partition`*`cloudfront::`*`account-id`*`:distribution/`*`distribution-id`*

- En el caso de un Equilibrador de carga de aplicación, el identificador corresponde al *`load-balancer-id`* en la sintaxis del ARN:

  `arn:`*`partition`*`:elasticloadbalancing:`*`region`*`:`*`account-id`*`:loadbalancer/app/`*`load-balancer-name/load-balancer-id`*

- En el caso de una API de REST de Amazon API Gateway, el identificador corresponde al *`api-id`* en la sintaxis del ARN:

  `arn:`*`partition`*`:apigateway:`*`region`*`::/restapis/`*`api-id`*`/stages/`*`stage-name`*

- Para una API de AWS AppSync GraphQL, el ID es el de *`GraphQLApiId`* la sintaxis del ARN:

`arn:partition:appsync:region:account-id:apis/GraphQLApiId`

- En el caso de un grupo de usuarios de Amazon Cognito, el identificador corresponde al *user-pool-id* en la sintaxis del ARN:

  `arn:partition:cognito-idp:region:account-id:userpool/user-pool-id`

- Para un AWS App Runner servicio, el ID es el de *apprunner-service-id* la sintaxis del ARN:

  `arn:partition:apprunner:region:account-id:service/apprunner-service-name/apprunner-service-id`

httpSourceName

El origen de la solicitud. Valores posibles: `CF` para Amazon CloudFront, `APIGW` para Amazon API Gateway, `ALB` para Application Load Balancer, `APPSYNC` para Amazon Cognito AWS AppSync`APPRUNNER`, `COGNITOIDP` para App Runner `VERIFIED_ACCESS` y para Verified Access.

httpVersion

La versión de HTTP.

ja3Fingerprint

La huella digital JA3 de la solicitud.

> **Note**
>
> La inspección de huellas dactilares JA3 solo está disponible para CloudFront las distribuciones de Amazon y los balanceadores de carga de aplicaciones.

La huella digital JA3 es un hash de 32 caracteres derivado del saludo del cliente TLS de una solicitud entrante. Esta huella digital sirve como identificador único para la configuración de TLS del cliente. AWS WAF calcula y registra esta huella digital para cada solicitud que contenga suficiente información de TLS Client Hello para el cálculo.

Este valor se proporciona al configurar una coincidencia de huellas digital JA3 en las reglas de la ACL web. Para obtener información sobre cómo crear una coincidencia con la huella digital JA3, consulte Huella digital JA3 en la Opciones de componentes de solicitudes para una instrucción de reglas.

etiquetas

Las etiquetas de la solicitud web. Estas etiquetas se aplicaban mediante reglas que se utilizaban para evaluar la solicitud. AWS WAF registra las primeras 100 etiquetas.

nonTerminatingMatchingReglas

La lista de reglas no terminantes que coincidían con la solicitud. Cada elemento de la lista contiene la siguiente información.

acción

La acción que AWS WAF se aplicó a la solicitud. Esto indica el recuento, el CAPTCHA o el desafío. Las CAPTCHA y Challenge son de no finalización cuando la solicitud web contiene un token válido.

ruleId

El ID de la regla que coincide con la solicitud y no era de finalización.

ruleMatchDetails

Información detallada sobre la regla que coincide con la solicitud. Este campo solo se rellena para las instrucciones de reglas de coincidencia de inyección de código SQL y scripting entre sitios (XSS). Una regla de coincidencia puede requerir una coincidencia para más de un criterio de inspección, por lo que estos detalles de coincidencia se proporcionan como una matriz de criterios de coincidencia.

La información adicional proporcionada para cada regla varía en función de factores como la configuración de la regla, el tipo de coincidencia de la regla y los detalles de la coincidencia. Por ejemplo, en el caso de las reglas con una CAPTCHA `captchaResponse` o una Challenge acción, `challengeResponse` aparecerá la o. Si la regla coincidente está en un grupo de reglas y has anulado la acción de regla configurada, la acción configurada aparecerá en. `overriddenAction`

oversizeFields

La lista de campos de la solicitud web que fueron inspeccionados por la ACL web y que superan el límite de AWS WAF inspección. Si un campo es demasiado grande pero la ACL web no lo inspecciona, no aparecerá aquí.

Esta lista puede contener cero o más de los siguientes valores: `REQUEST_BODY`, `REQUEST_JSON_BODY`, `REQUEST_HEADERS` y `REQUEST_COOKIES`. Para obtener más

información acerca de los campos sobredimensionados, consulte Manejo de componentes de solicitudes sobredimensionadas en AWS WAF.

rateBasedRuleLista

La lista de reglas basadas en frecuencia que actuaron en la solicitud. Para obtener información acerca de las reglas basadas en tasas, consulte Instrucción de regla basada en frecuencia.

rateBasedRuleID

El ID de la regla basada en frecuencia que actuó en la solicitud. Si esto ha terminado la solicitud, el ID de `rateBasedRuleId` es el mismo que el ID de `terminatingRuleId`.

rateBasedRuleNombre

El nombre de la regla basada en tasas que actuó en la solicitud.

limitKey

El tipo de agregación que utiliza la regla. Los valores posibles son `IP` para el origen de la solicitud web, `FORWARDED_IP` para una IP reenviada en un encabezado de la solicitud, `CUSTOMKEYS` para la configuración personalizada de las claves agregadas y `CONSTANT` para el recuento conjunto de todas las solicitudes, sin agregación.

limitValue

Se usa solo cuando se limita la tasa a un solo tipo de dirección IP. Si una solicitud contiene una dirección IP que no es válida, el `limitvalue` es `INVALID`.

maxRateAllowed

El número máximo de solicitudes permitidas en el intervalo de tiempo especificado para una instancia de agregación específica. La instancia de agregación se define mediante `limitKey` las especificaciones clave adicionales que haya proporcionado en la configuración de reglas basadas en tasas.

evaluationWindowSec

La cantidad de tiempo AWS WAF incluida en su solicitud se cuenta, en segundos.

customValues

Valores únicos identificados por la regla basada en tasas de la solicitud. En el caso de los valores de cadena, los registros imprimen los primeros 32 caracteres del valor de cadena. Según el tipo de clave, estos valores pueden ser solo para una clave, como para un método

HTTP o una cadena de consulta, o pueden ser para una clave y un nombre, como para el encabezado y el nombre del encabezado.

requestHeadersInserted

La lista de encabezados insertados para la gestión personalizada de las solicitudes.

ID de solicitud

El ID de la solicitud, que es generado por el servicio de alojamiento subyacente. Para el equilibrador de carga de aplicación, este es el identificador de rastro. Para el resto, este el el identificador de la solicitud.

responseCodeSent

El código de respuesta enviado con una respuesta personalizada.

ruleGroupId

El ID del grupo de reglas. Si la regla bloqueó la solicitud, el ID de `ruleGroupID` es el mismo que el ID de `terminatingRuleId`.

ruleGroupList

La lista de grupos de reglas que actuaron en esta solicitud, que coinciden con la información.

terminatingRule

La regla que terminó la solicitud. Si está presente, contiene la siguiente información.

acción

La acción de finalización que AWS WAF se aplicó a la solicitud. Esto indica permitir, bloquear, CAPTCHA o desafío. Las acciones CAPTCHA y Challenge son de finalización cuando la solicitud web no contiene un token válido.

ruleId

El identificador de la regla que coincide con la solicitud.

ruleMatchDetails

Información detallada sobre la regla que coincide con la solicitud. Este campo solo se rellena para las instrucciones de reglas de coincidencia de inyección de código SQL y scripting entre sitios (XSS). Una regla de coincidencia puede requerir una coincidencia para más de un criterio de inspección, por lo que estos detalles de coincidencia se proporcionan como una matriz de criterios de coincidencia.

La información adicional proporcionada para cada regla varía en función de factores como la configuración de la regla, el tipo de coincidencia de la regla y los detalles de la coincidencia. Por ejemplo, en el caso de las reglas con una CAPTCHA `captchaResponse` o una Challenge acción, `challengeResponse` aparecerá la o. Si la regla coincidente está en un grupo de reglas y has anulado la acción de regla configurada, la acción configurada aparecerá en. `overriddenAction`

terminatingRuleId

El ID de la regla que terminó la solicitud. Si nada termina la solicitud, el valor es `Default_Action`.

terminatingRuleMatchDetalles

Información detallada sobre la regla de finalización que coincide con la solicitud. Una regla de finalización tiene una acción que finaliza el proceso de inspección ante una solicitud web. Entre las posibles acciones de una regla de finalización se incluyen Allow, Block, CAPTCHA y Challenge. Durante la inspección de una solicitud web, la primera regla que coincida con la solicitud y que tenga una acción de finalización, AWS WAF detiene la inspección y aplica la acción. La solicitud web puede contener otras amenazas, además de la que aparece en el registro de la regla de finalización coincidente.

Esto solo se rellena para las instrucciones de reglas de coincidencia de inyección de código SQL y scripting entre sitios (XSS). La regla de coincidencia puede requerir una coincidencia para más de un criterio de inspección, por lo que estos detalles de coincidencia se proporcionan como una matriz de criterios de coincidencia.

terminatingRuleType

El tipo de regla que terminó la solicitud. Valores posibles: RATE_BASED, REGULAR, GROUP y MANAGED_RULE_GROUP.

Marca de tiempo

La marca de tiempo en milisegundos.

uri

El URI de la solicitud.

webaclId

El GUID de la ACL web.

Ejemplos de registro

Example Regla basada en tasas 1: configuración de la regla con una clave, establecida en **`Header:dogname`**

```
    {
      "Name": "RateBasedRule",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 100,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
            {
              "Header": {
                "Name": "dogname",
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "RateBasedRule"
      }
    }
```

Example Regla basada en tasas 1: entrada de registro de la solicitud bloqueada por la regla basada en tasas

```
{
   "timestamp":1683355579981,
```

```
    "formatVersion":1,
    "webaclId": ...,
    "terminatingRuleId":"RateBasedRule",
    "terminatingRuleType":"RATE_BASED",
    "action":"BLOCK",
    "terminatingRuleMatchDetails":[

    ],
    "httpSourceName":"APIGW",
    "httpSourceId":"EXAMPLE11:rjvegx5guh:CanaryTest",
    "ruleGroupList":[

    ],
    "rateBasedRuleList":[
       {
          "rateBasedRuleId": ...,
          "rateBasedRuleName":"RateBasedRule",
          "limitKey":"CUSTOMKEYS",
          "maxRateAllowed":100,
          "evaluationWindowSec":"120",
          "customValues":[
             {
                "key":"HEADER",
                "name":"dogname",
                "value":"ella"
             }
          ]
       }
    ],
    "nonTerminatingMatchingRules":[

    ],
    "requestHeadersInserted":null,
    "responseCodeSent":null,
    "httpRequest":{
       "clientIp":"52.46.82.45",
       "country":"FR",
       "headers":[
          {
             "name":"X-Forwarded-For",
             "value":"52.46.82.45"
          },
          {
             "name":"X-Forwarded-Proto",
```

```
            "value":"https"
         },
         {
            "name":"X-Forwarded-Port",
            "value":"443"
         },
         {
            "name":"Host",
            "value":"rjvegx5guh.execute-api.eu-west-3.amazonaws.com"
         },
         {
            "name":"X-Amzn-Trace-Id",
            "value":"Root=1-645566cf-7cb058b04d9bb3ee01dc4036"
         },
         {
            "name":"dogname",
            "value":"ella"
         },
         {
            "name":"User-Agent",
            "value":"RateBasedRuleTestKoipOneKeyModulePV2"
         },
         {
            "name":"Accept-Encoding",
            "value":"gzip,deflate"
         }
      ],
      "uri":"/CanaryTest",
      "args":"",
      "httpVersion":"HTTP/1.1",
      "httpMethod":"GET",
      "requestId":"Ed0AiHF_CGYF-DA="
   }
}
```

Example Regla basada en tasas 2: configuración de la regla con dos claves, establecidas en **`Header:dogname`** y **`Header:catname`**

```
    {
      "Name": "RateBasedRule",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
```

```
          "Limit": 100,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
            {
              "Header": {
                "Name": "dogname",
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            },
            {
              "Header": {
                "Name": "catname",
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "RateBasedRule"
      }
    }
```

Example Regla basada en tasas 2: entrada de registro de la solicitud bloqueada por la regla basada en tasas

```
{
   "timestamp":1633322211194,
```

```
    "formatVersion":1,
    "webaclId":...,
    "terminatingRuleId":"RateBasedRule",
    "terminatingRuleType":"RATE_BASED",
    "action":"BLOCK",
    "terminatingRuleMatchDetails":[

    ],
    "httpSourceName":"APIGW",
    "httpSourceId":"EXAMPLE11:rjvegx5guh:CanaryTest",
    "ruleGroupList":[

    ],
    "rateBasedRuleList":[
       {
          "rateBasedRuleId":...,
          "rateBasedRuleName":"RateBasedRule",
          "limitKey":"CUSTOMKEYS",
          "maxRateAllowed":100,
          "evaluationWindowSec":"120",
          "customValues":[
             {
                "key":"HEADER",
                "name":"dogname",
                "value":"ella"
             },
             {
                "key":"HEADER",
                "name":"catname",
                "value":"goofie"
             }
          ]
       }
    ],
    "nonTerminatingMatchingRules":[

    ],
    "requestHeadersInserted":null,
    "responseCodeSent":null,
    "httpRequest":{
       "clientIp":"52.46.82.35",
       "country":"FR",
       "headers":[
          {
```

```
            "name":"X-Forwarded-For",
            "value":"52.46.82.35"
         },
         {
            "name":"X-Forwarded-Proto",
            "value":"https"
         },
         {
            "name":"X-Forwarded-Port",
            "value":"443"
         },
         {
            "name":"Host",
            "value":"23llbyn8v3.execute-api.eu-west-3.amazonaws.com"
         },
         {
            "name":"X-Amzn-Trace-Id",
            "value":"Root=1-64556629-17ac754c2ed9f0620e0f2a0c"
         },
         {
            "name":"catname",
            "value":"goofie"
         },
         {
            "name":"dogname",
            "value":"ella"
         },
         {
            "name":"User-Agent",
            "value":"Apache-HttpClient/UNAVAILABLE (Java/11.0.19)"
         },
         {
            "name":"Accept-Encoding",
            "value":"gzip,deflate"
         }
      ],
      "uri":"/CanaryTest",
      "args":"",
      "httpVersion":"HTTP/1.1",
      "httpMethod":"GET",
      "requestId":"EdzmlH5OCGYF1vQ="
   }
}
```

Example Resultado de registro de una regla que se activó al detectar SQLi (finalización)

```
{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/
STMTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "HIGH",
            "location": "HEADER",
            "matchedData": [
                "10",
                "AND",
                "1"
            ]
        }
    ],
    "httpSourceName": "-",
    "httpSourceId": "-",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
        "headers": [
            {
                "name": "Host",
                "value": "localhost:1989"
            },
            {
                "name": "User-Agent",
                "value": "curl/7.61.1"
            },
            {
                "name": "Accept",
                "value": "*/*"
            },
            {
```

```
                "name": "x-stm-test",
                "value": "10 AND 1=1"
            }
        ],
        "uri": "/myUri",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "GET",
        "requestId": "rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example Resultado de registro de una regla que se activó al detectar SQLi (sin finalización)

```
{
    "timestamp":1592357192516
    ,"formatVersion":1
    ,"webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"Default_Action"
    ,"terminatingRuleType":"REGULAR"
    ,"action":"ALLOW"
    ,"terminatingRuleMatchDetails":[]
    ,"httpSourceName":"-"
    ,"httpSourceId":"-"
    ,"ruleGroupList":[]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":
    [{
        "ruleId":"TestRule"
        ,"action":"COUNT"
        ,"ruleMatchDetails":
        [{
            "conditionType":"SQL_INJECTION"
            ,"sensitivityLevel": "HIGH"
            ,"location":"HEADER"
            ,"matchedData":[
                "10"
```

```
                ,"and"
                ,"1"]
            }]
    }]
    ,"httpRequest":{
        "clientIp":"3.3.3.3"
        ,"country":"US"
        ,"headers":[
            {"name":"Host","value":"localhost:1989"}
            ,{"name":"User-Agent","value":"curl/7.61.1"}
            ,{"name":"Accept","value":"*/*"}
            ,{"name":"myHeader","myValue":"10 AND 1=1"}
            ]
            ,"uri":"/myUri","args":""
            ,"httpVersion":"HTTP/1.1"
            ,"httpMethod":"GET"
            ,"requestId":"rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example Resultado de registro de varias reglas que se activaron dentro de un grupo de reglas (RuleA-XSS es de finalización y la Rule-B, no)

```
{
    "timestamp":1592361810888,
    "formatVersion":1,
    "webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"RG-Reference"
    ,"terminatingRuleType":"GROUP"
    ,"action":"BLOCK",
    "terminatingRuleMatchDetails":
    [{
        "conditionType":"XSS"
        ,"location":"HEADER"
        ,"matchedData":["<","frameset"]
    }]
    ,"httpSourceName":"-"
```

```
    ,"httpSourceId":"-"
    ,"ruleGroupList":
    [{
        "ruleGroupId":"arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/hello-
world/c05lb698-1f11-4m41-aef4-99a506d53f4b"
        ,"terminatingRule":{
            "ruleId":"RuleA-XSS"
            ,"action":"BLOCK"
            ,"ruleMatchDetails":null
            }
        ,"nonTerminatingMatchingRules":
        [{
            "ruleId":"RuleB-SQLi"
            ,"action":"COUNT"
            ,"ruleMatchDetails":
            [{
                "conditionType":"SQL_INJECTION"
                ,"sensitivityLevel": "LOW"
                ,"location":"HEADER"
                ,"matchedData":[
                    "10"
                    ,"and"
                    ,"1"]
            }]
        }]
        ,"excludedRules":null
    }]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":[]
    ,"httpRequest":{
        "clientIp":"3.3.3.3"
        ,"country":"US"
        ,"headers":
        [
            {"name":"Host","value":"localhost:1989"}
            ,{"name":"User-Agent","value":"curl/7.61.1"}
            ,{"name":"Accept","value":"*/*"}
            ,{"name":"myHeader1","value":"<frameset onload=alert(1)>"}
            ,{"name":"myHeader2","value":"10 AND 1=1"}
            ]
        ,"uri":"/myUri"
        ,"args":""
        ,"httpVersion":"HTTP/1.1"
        ,"httpMethod":"GET"
```

```
        ,"requestId":"rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example Resultado de registro de una regla que se activó para inspeccionar el cuerpo de la solicitud con el tipo de contenido JSON

AWS WAF actualmente informa que la ubicación de la inspección corporal de JSON es`UNKNOWN`.

```
{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:123456789012:regional/webacl/test/111",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "LOW",
            "location": "UNKNOWN",
            "matchedData": [
                "10",
                "AND",
                "1"
            ]
        }
    ],
    "httpSourceName": "ALB",
    "httpSourceId": "alb",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
    "requestHeadersInserted":null,
    "responseCodeSent":null,
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
```

```
        "headers": [],
        "uri": "",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "POST",
        "requestId": "null"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example Resultado de registro de una regla de CAPTCHA para una solicitud web con un token de CAPTCHA válido y vigente

La siguiente lista de registros corresponde a una solicitud web que asoció una regla con una acción CAPTCHA. La solicitud web tiene un token de CAPTCHA válido y no caducado, y solo se anota cuando coincide con el CAPTCHA AWS WAF, de forma similar al comportamiento de la acción. Count Esta coincidencia de CAPTCHA se indica en `nonTerminatingMatchingRules`.

```
{
  "timestamp": 1632420429309,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-
acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [
    {
      "ruleId": "captcha-rule",
      "action": "CAPTCHA",
      "ruleMatchDetails": [],
      "captchaResponse": {
        "responseCode": 0,
        "solveTimestamp": 1632420429
```

```
      }
    }
  ],
  "requestHeadersInserted": [
    {
      "name": "x-amzn-waf-test-header-name",
      "value": "test-header-value"
    }
  ],
  "responseCodeSent": null,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "72.21.198.65"
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc24d-5ad89a09181910c43917a888"
      },
      {
        "name": "cache-control",
        "value": "max-age=0"
      },
      {
        "name": "sec-ch-ua",
        "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand
\";v=\"99\""
      },
      {
```

```
        "name": "sec-ch-ua-mobile",
        "value": "?0"
      },
      {
        "name": "sec-ch-ua-platform",
        "value": "\"Windows\""
      },
      {
        "name": "upgrade-insecure-requests",
        "value": "1"
      },
      {
        "name": "user-agent",
        "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/94.0.4606.54 Safari/537.36"
      },
      {
        "name": "accept",
        "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
      },
      {
        "name": "sec-fetch-site",
        "value": "same-origin"
      },
      {
        "name": "sec-fetch-mode",
        "value": "navigate"
      },
      {
        "name": "sec-fetch-user",
        "value": "?1"
      },
      {
        "name": "sec-fetch-dest",
        "value": "document"
      },
      {
        "name": "referer",
        "value": "https://b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com/pen-
test/pets"
      },
      {
        "name": "accept-encoding",
```

```
        "value": "gzip, deflate, br"
      },
      {
        "name": "accept-language",
        "value": "en-US,en;q=0.9"
      },
      {
        "name": "cookie",
        "value": "aws-waf-token=51c71352-41f5-4f6d-b676-c24907bdf819:EQoAZ/J
+AAQAAAAA:t9wvxbw042wva7E2Y6lgud/
bS6YG0CJKVAJqaRqDZ140ythKW0Zj9wKB2O8lSkYDRqf1yONcVBFo5u0eYi0tvT4rtQCXsu
+KanAardW8go4QSLw4yoED59lgV7oAhGyCalAzE7ra29j+RvvZPsQyoQuDCrtoY/TvQyMTXIXzGPDC/rKBbg=="
      }
    ],
    "uri": "/pen-test/pets",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "GINMHHUgoAMFxug="
  }
}
```

Example Resultado de registro de una regla de CAPTCHA para una solicitud web que no tiene un token de CAPTCHA

La siguiente lista de registros corresponde a una solicitud web que asoció una regla con una acción CAPTCHA. La solicitud web no tenía un token CAPTCHA y estaba bloqueada por. AWS WAF

```
{
  "timestamp": 1632420416512,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-
acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "captcha-rule",
  "terminatingRuleType": "REGULAR",
  "action": "CAPTCHA",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [],
  "requestHeadersInserted": null,
```

```
  "responseCodeSent": 405,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "72.21.198.65"
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc240-18b57ff33c10e5c016b508c5"
      },
      {
        "name": "sec-ch-ua",
        "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand
\";v=\"99\""
      },
      {
        "name": "sec-ch-ua-mobile",
        "value": "?0"
      },
      {
        "name": "sec-ch-ua-platform",
        "value": "\"Windows\""
      },
      {
        "name": "upgrade-insecure-requests",
        "value": "1"
      },
      {
        "name": "user-agent",
```

```
        "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/94.0.4606.54 Safari/537.36"
      },
      {
        "name": "accept",
        "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
      },
      {
        "name": "sec-fetch-site",
        "value": "cross-site"
      },
      {
        "name": "sec-fetch-mode",
        "value": "navigate"
      },
      {
        "name": "sec-fetch-user",
        "value": "?1"
      },
      {
        "name": "sec-fetch-dest",
        "value": "document"
      },
      {
        "name": "accept-encoding",
        "value": "gzip, deflate, br"
      },
      {
        "name": "accept-language",
        "value": "en-US,en;q=0.9"
      }
    ],
    "uri": "/pen-test/pets",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "GINKHEssoAMFsrg="
  },
  "captchaResponse": {
    "responseCode": 405,
    "solveTimestamp": 0,
    "failureReason": "TOKEN_MISSING"
  }
```

```
}
```

Probando y ajustando sus AWS WAF protecciones

Le recomendamos que pruebe y ajuste los cambios en su ACL AWS WAF web antes de aplicarlos al tráfico de su sitio web o aplicación web.

> ⚠ Riesgo de tráfico de producción
>
> Antes de implementar cambios en su ACL web para el tráfico de producción, pruébelos y ajústelos en un entorno provisional o de prueba hasta que se sienta cómodo con el posible impacto en el tráfico. A continuación, pruebe y ajuste las reglas en el modo de recuento con el tráfico de producción antes de habilitarlas.

En esta sección se proporcionan instrucciones para probar y ajustar las ACL AWS WAF web, las reglas, los grupos de reglas, los conjuntos de IP y los conjuntos de patrones de expresiones regulares.

En esta sección, también se proporcionan instrucciones generales para probar el uso de grupos de reglas administrados por otra persona. Estos incluyen los grupos de reglas AWS AWS Marketplace administradas, los grupos de reglas administradas y los grupos de reglas que otra cuenta comparte con usted. Para estos grupos de reglas, siga también las instrucciones que le dé el proveedor del grupo de reglas.

- Para ver el grupo de reglas AWS administradas de control de bots, consulte tambiénPrueba e implementación de AWS WAF Bot Control.
- Para ver el grupo de reglas de reglas AWS administradas para prevenir la apropiación de cuentas, consulte Pruebas e implementación de la ATP también.
- Para ver el grupo de reglas AWS administradas para la prevención del fraude en la creación de cuentas, consulte Pruebas implementación de la ACFP también.

Incoherencias temporales durante las actualizaciones

Al crear o cambiar una ACL web u otros AWS WAF recursos, los cambios tardan un poco en propagarse a todas las áreas donde se almacenan los recursos. El tiempo de propagación puede oscilar entre unos segundos y varios minutos.

A continuación, se proporcionan ejemplos de incoherencias temporales que podría notar durante la propagación de los cambios:

- Después de crear una ACL web, si intenta asociarla a un recurso, es posible que se produzca una excepción que indique que la ACL web no está disponible.
- Después de agregar un grupo de reglas a una ACL web, las nuevas reglas del grupo de reglas pueden estar en vigor en un área en la que se usa la ACL web y no en otra.
- Tras cambiar la configuración de una acción de regla, es posible que vea la acción anterior en algunos lugares y la acción nueva en otros.
- Después de agregar una dirección IP a un conjunto de IP que está en uso dentro de una regla de bloqueo, es posible que la nueva dirección se bloquee en un área, pero que se permita en otra.

Comprobación y ajuste de los pasos de alto nivel

Esta sección proporciona una lista de verificación de los pasos para probar los cambios en la ACL web, incluidas las reglas o grupos de reglas que utilice.

> **Note**
>
> Para seguir las instrucciones de esta sección, debe comprender cómo crear y administrar protecciones de AWS WAF , como las ACL web, las reglas y los grupos de reglas. Esta información se describe en secciones anteriores de esta guía.

Prueba y ajuste de su ACL web

Realice estos pasos primero en un entorno de prueba y, después, en producción.

1. Preparativos para la prueba

   Prepare su entorno de supervisión, cambie sus nuevas AWS WAF protecciones al modo de recuento para realizar pruebas y cree las asociaciones de recursos que necesite.

   Consulte Preparación para las pruebas.

2. Monitorización y ajuste de los entornos de prueba y producción

   Supervise y ajuste sus AWS WAF protecciones primero en un entorno de prueba o ensayo y, después, en producción, hasta que esté convencido de que pueden gestionar el tráfico tal y como lo necesita.

   Consulte Monitorización y ajuste.

3. Habilitación de sus protecciones en la producción

   Cuando esté satisfecho con las protecciones de prueba, cámbielas al modo de producción, elimine los artefactos de prueba innecesarios y continúe con la monitorización.

   Consulte Habilitación de sus protecciones en la producción.

Cuando haya terminado de implementar los cambios, continúe monitorizando el tráfico web y las protecciones en producción para asegurarse de que funcionan como desee. Los patrones de tráfico web pueden cambiar con el tiempo, por lo que es posible que tenga que ajustar las protecciones de vez en cuando.

Preparación para las pruebas

En esta sección se describe cómo prepararse para probar y ajustar sus AWS WAF protecciones.

> **Note**
>
> Para seguir las instrucciones de esta sección, debe comprender en general cómo crear y administrar AWS WAF protecciones, como las ACL web, las reglas y los grupos de reglas. Esta información se describe en secciones anteriores de esta guía.

Prepararse para la prueba

1. Habilite el registro de ACL web, CloudWatch las métricas de Amazon y el muestreo de solicitudes web para la ACL web

   Utilice el registro, las métricas y el muestreo para monitorizar la interacción de las reglas de la ACL web con el tráfico web.

- Registro: puede configurarlo AWS WAF para registrar las solicitudes web que evalúa una ACL web. Puede enviar registros a CloudWatch registros, a un bucket de Amazon S3 o a una transmisión de entrega de Amazon Data Firehose. Puede redactar campos y aplicar filtros. Para obtener más información, consulte Registro del tráfico de ACL AWS WAF web.
- Amazon Security Lake: puede configurar Security Lake para recopilar datos de ACL web. Security Lake recopila datos de registros y eventos de diversas fuentes para su normalización, análisis y administración. Para obtener información sobre esta opción, consulte ¿Qué es Amazon Security Lake? y Recopilación de datos de AWS los servicios de la guía del usuario de Amazon Security Lake.
- CloudWatch Métricas de Amazon: en su configuración de ACL web, proporcione especificaciones métricas para todo lo que desee monitorear. Puede ver las métricas a través de las CloudWatch consolas AWS WAF y. Para obtener más información, consulte Monitorización con Amazon CloudWatch.
- Muestreo de solicitudes web: puede ver una muestra de todas las solicitudes web que evalúa la ACL web. Para obtener información sobre cómo el muestreo de las solicitudes de web, consulte Visualizar una muestra de solicitudes web.

2. Configuración de las protecciones en modo Count

   En su configuración de ACL web, cambie todo lo que desee probar al modo de recuento. Esto hace que las protecciones de prueba registren las coincidencias con las solicitudes web sin alterar la forma en que se gestionan las solicitudes. Podrá ver las coincidencias en sus métricas, registros y solicitudes muestreadas para verificar los criterios de coincidencia y comprender cuáles podrían ser los efectos en el tráfico web. Las reglas que agregan etiquetas a las solicitudes coincidentes agregarán etiquetas independientemente de la acción de regla.

   - Regla definida en la ACL web: edite las reglas de la ACL web y defina sus acciones en Count.
   - Grupo de reglas: en su configuración de ACL web, edite la instrucción de reglas del grupo de reglas y, en el panel Reglas, abra el menú desplegable Anular todas las acciones de regla y elija Count. Si administra la ACL web en JSON, agregue las reglas a la configuración `RuleActionOverrides` de la instrucción de referencia del grupo de reglas, con `ActionToUse` establecido en Count. En la siguiente lista de ejemplos, se muestran las anulaciones de dos reglas del grupo de reglas `AWSManagedRulesAnonymousIpList` AWS administradas.

     ```
     "ManagedRuleGroupStatement": {
       "VendorName": "AWS",
     ```

```
    "Name": "AWSManagedRulesAnonymousIpList",
      "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "AnonymousIPList"
        },
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "HostingProviderIPList"
        }
      ],
      "ExcludedRules": []
    }
  },
```

Para obtener más información sobre la anulación de las acciones de las reglas, consulte Invalidar acciones de reglas en un grupo de reglas.

Para su propio grupo de reglas, no modifique las acciones de regla en el propio grupo de reglas. Las reglas de los grupos de reglas con acción Count no generan las métricas u otros artefactos que se necesitan para las pruebas. Además, cambiar un grupo de reglas afecta a todas las ACL web que lo utilizan, mientras que los cambios en la configuración de las ACL web solo afectan a esa ACL web única.

- ACL web: si está probando una nueva ACL web, defina la acción predeterminada para que la ACL web permita las solicitudes. Esto le permite probar la ACL web sin afectar al tráfico de ninguna manera.

En general, el modo de recuento genera más coincidencias que el de producción. Esto se debe a que una regla que cuenta las solicitudes no detiene la evaluación de la solicitud por parte de la ACL web, por lo que las reglas que se ejecutan más adelante en la ACL web también pueden coincidir con la solicitud. Cuando cambie las acciones de regla a su configuración de producción, las reglas que permiten o bloquean las solicitudes finalizarán la evaluación de las solicitudes que coincidan. Como resultado, las solicitudes coincidentes generalmente se inspeccionarán mediante un menor número de reglas en la ACL web. Para obtener más información acerca

de los efectos de las acciones de regla en la evaluación general de una solicitud web, consulte Acción de regla.

Con esta configuración, las nuevas protecciones no alterarán el tráfico web, sino que generarán información de coincidencia en las métricas, los registros de ACL web y los ejemplos de solicitudes.

3. Asocie la ACL web con un recurso

   Si la ACL web aún no está asociada al recurso, asóciela.

   Consulte Asociar o desasociar una ACL web a un recurso AWS.

Ahora está listo para monitorizar y ajustar la ACL web.

Monitorización y ajuste

En esta sección se describe cómo supervisar y ajustar AWS WAF las protecciones.

> **Note**
>
> Para seguir las instrucciones de esta sección, debe comprender en general cómo crear y administrar AWS WAF protecciones, como las ACL web, las reglas y los grupos de reglas. Esta información se describe en secciones anteriores de esta guía.

Supervise el tráfico web y las coincidencias de reglas para verificar el comportamiento de la ACL web. Si encuentra problemas, ajuste las reglas para corregirlas y, a continuación, supervise para verificar los ajustes.

Repita el siguiente procedimiento hasta que la ACL web administre su tráfico web como lo necesite.

Monitorizar y ajustar

1. Supervise el tráfico y las coincidencias de reglas

   Asegúrese de que el tráfico fluya y de que las reglas de prueba encuentren solicitudes coincidentes.

   Busque la siguiente información sobre las protecciones que está probando:

- Registros: acceda a la información sobre las reglas que coinciden con una solicitud web:
  - Sus reglas: las reglas de la ACL web que requieren la acción Count se enumeran en `nonTerminatingMatchingRules`. Las reglas con Allow o Block se enumeran en `terminatingRule`. Las reglas con CAPTCHA o Challenge pueden ser de finalización o no, y, por lo tanto, se incluyen en una de las dos categorías, según el resultado de la coincidencia de reglas.
  - Grupos de reglas: los grupos de reglas se identifican en el campo `ruleGroupId` y sus coincidencias de reglas se clasifican de la misma manera que en el caso de las reglas independientes.
  - Etiquetas: las etiquetas que las reglas han aplicado a la solicitud aparecen en el campo `Labels`.

  Para obtener más información, consulte Campos de registro.
- CloudWatch Métricas de Amazon: puede acceder a las siguientes métricas para evaluar su solicitud de ACL web.
  - Sus reglas: las métricas se agrupan según la acción de la regla. Por ejemplo, cuando pruebas una regla en Count modo, sus coincidencias se muestran como `Count` métricas para la ACL web.
  - Sus grupos de reglas: las métricas de sus grupos de reglas se muestran en las métricas del grupo de reglas.
  - Grupos de reglas que pertenecen a otra cuenta: las métricas de los grupos de reglas, por lo general, solo las puede ver el propietario del grupo de reglas. Sin embargo, si anulas la acción de la regla para una regla, las métricas de esa regla aparecerán en las métricas de tu ACL web. Además, las etiquetas agregadas por cualquier grupo de reglas aparecen en las métricas de su ACL web

    Los grupos de reglas de esta categoría son AWS Reglas administradas para AWS WAF AWS Marketplace grupos de reglas gestionadosGrupos de reglas proporcionados por otros servicios, y los grupos de reglas que otra cuenta comparte contigo.
  - Etiquetas: las etiquetas que se agregaron a una solicitud web durante la evaluación aparecen en las métricas de etiquetas de la ACL web. Puede acceder a las métricas de todas las etiquetas, independientemente de si las han agregado sus reglas y grupos de reglas o si las han agregado las reglas de un grupo de reglas propiedad de otra cuenta.

  Para obtener más información, consulte Visualización de las métricas para la ACL web.

- Paneles de información general sobre el tráfico de las ACL web: para acceder a los resúmenes del tráfico web que ha evaluado una ACL web, vaya a la página de la ACL web en la AWS WAF consola y abra la pestaña de información general del tráfico.

  Los paneles de información general del tráfico proporcionan resúmenes casi en tiempo real de CloudWatch las métricas de Amazon que AWS WAF recopila cuando evalúa el tráfico web de tu aplicación.

  Para obtener más información, consulte Paneles de información general sobre el tráfico de ACL web.
- Solicitudes web muestreadas: acceda a la información de las reglas que coinciden con una muestra de solicitudes web. La información de muestra identifica las reglas coincidentes por el nombre de la métrica de la regla en la ACL web. En el caso de los grupos de reglas, la métrica identifica la instrucción de referencia del grupo de reglas. En el caso de las reglas incluidas en los grupos de reglas, la muestra indica el nombre de la regla coincidente en `RuleWithinRuleGroup`.

  Para obtener más información, consulte Visualizar una muestra de solicitudes web.

2. Configuración de las mitigaciones para abordar los falsos positivos

   Si determina que una regla genera falsos positivos, al hacer coincidir las solicitudes web cuando no debería, las siguientes opciones pueden ayudarle a ajustar las protecciones de las ACL web para mitigarlos.

   Corrección de los criterios de inspección de las reglas

   Para sus propias reglas, a menudo solo necesita ajustar la configuración que utiliza para inspeccionar las solicitudes web. Algunos ejemplos incluyen cambiar las especificaciones de un conjunto de patrones de regex, ajustar las transformaciones de texto que se aplican a un componente de la solicitud antes de la inspección o cambiar a una dirección IP reenviada. Consulte la guía sobre el tipo de regla que está causando problemas en Conceptos básicos de las instrucciones de regla.

   Corrección de problemas más complejos

   En el caso de los criterios de inspección que no controla y de algunas reglas complejas, es posible que tenga que realizar otros cambios, como agregar reglas que permitan o bloqueen las solicitudes de forma explícita, o que eliminen las solicitudes de la evaluación por la regla problemática. Los grupos de reglas administrados suelen necesitar este tipo de mitigación,

pero otras reglas, también. Los ejemplos incluyen la instrucción de regla basada en tasas y la instrucción de reglas de los ataques de inyección de código SQL.

Lo que haga para mitigar los falsos positivos depende de su caso de uso. A continuación, se muestran algunos enfoques comunes:

- Añadir una regla de mitigación: añada una regla que se ejecute antes que la nueva regla y que permita de forma explícita las solicitudes que provoquen falsos positivos. Para obtener más información sobre el orden de evaluación de las reglas en una ACL web, consulte Procesamiento del orden de las reglas y los grupos de reglas en una ACL web.

  Con este enfoque, las solicitudes permitidas se envían al recurso protegido, por lo que nunca llegan a la nueva regla para su evaluación. Si la nueva regla es un grupo de reglas administrado de pago, este enfoque también puede ayudar a contener el coste de usar el grupo de reglas.
- Agregar una regla lógica con una regla de mitigación: utilice enunciados de reglas lógicas para combinar la nueva regla con una regla que excluya los falsos positivos. Para obtener más información, consulte instrucciones de reglas lógicas.

  Por ejemplo, supongamos que va a agregar una instrucción de coincidencia de un ataque de inyección de código SQL que genera falsos positivos para una categoría de solicitudes. Cree una regla que coincida con esas solicitudes y, a continuación, combine las reglas mediante instrucciones de reglas lógicas para que solo coincidan con las solicitudes que no coincidan con los criterios de falsos positivos y sí con los criterios de ataque de inyección de código SQL.
- Agregar una instrucción de restricción de acceso: en el caso de las instrucciones basadas en tasas y las instrucciones de referencia de grupos de reglas administrados, excluya de la evaluación las solicitudes que den como resultado falsos positivos agregando una instrucción de restricción de acceso dentro de la instrucción principal.

  Las solicitudes que no coincidan con la instrucción de restricción de acceso nunca llegan al grupo de reglas ni a la evaluación basada en tasas. Para obtener información sobre las instrucciones de restricción de acceso, consulte Instrucciones de restricción de acceso. Para ver un ejemplo, consulte Exclusión del rango de IP de la administración de bots.
- Agregar una regla de coincidencia de etiquetas: en el caso de los grupos de reglas que utilizan el etiquetado, identifique la etiqueta que la regla problemática aplica a las solicitudes. Es posible que primero deba configurar las reglas del grupo de reglas en el modo de recuento si aún no lo ha hecho. Añada una regla de coincidencia de etiquetas, posicionada de forma

que se ejecute después del grupo de reglas, que coincida con la etiqueta que está agregando la regla problemática. En la regla de coincidencia de etiquetas, puede filtrar las solicitudes que quiere permitir de las que quiere bloquear.

Si utiliza este enfoque, cuando termine de realizar las pruebas, mantenga la regla problemática en modo de recuento en el grupo de reglas y conserve su regla de coincidencia de etiquetas personalizada. Para obtener información sobre las instrucciones del control de bots, consulte Instrucción de regla de coincidencia de etiquetas. Para ver ejemplos, consulte Permisión de un bot bloqueado específico y Ejemplo de ATP: gestión personalizada de las credenciales faltantes o comprometidas.

- Cambiar la versión de un grupo de reglas administrado: en el caso de los grupos de reglas administrados con control de versiones, cambie la versión que esté usando. Por ejemplo, puede volver a la última versión estática que utilizó correctamente.

  Por lo general, se trata de una solución temporal. Puede cambiar la versión de su tráfico de producción mientras continúa probando la última versión en su entorno de prueba o ensayo, o mientras espera a que el proveedor proporcione una versión más compatible. Para obtener información acerca de las versiones de los grupos de reglas administrados, consulte Grupos de reglas administrados.

Cuando esté seguro de que las nuevas reglas coinciden con las solicitudes que necesita, pase a la siguiente fase de las pruebas y repita este procedimiento. Realice la fase final de pruebas y ajustes en su entorno de producción.

Visualización de las métricas para la ACL web

Una vez que hayas asociado una ACL web a uno o más AWS recursos, puedes ver las métricas resultantes de la asociación en un CloudWatch gráfico de Amazon.

Para obtener información sobre AWS WAF las métricas, consulteAWS WAF métricas y dimensiones. Para obtener información sobre CloudWatch las métricas, consulta la Guía del CloudWatch usuario de Amazon.

Para cada una de las reglas de una ACL web y para todas las solicitudes a las que se reenvía un recurso asociado AWS WAF para una ACL web CloudWatch , puede hacer lo siguiente:

- Ver los datos correspondientes a la hora anterior o a las tres horas anteriores.
- Cambiar el intervalo entre puntos de datos.

- Cambie el cálculo que se CloudWatch realiza con los datos, como el máximo, el mínimo, el promedio o la suma.

> **Note**
>
> AWS WAF with CloudFront es un servicio global y las métricas solo están disponibles si eliges la región EE. UU. Este (Virginia del Norte) en AWS Management Console. Si eliges otra región, no aparecerá ninguna AWS WAF métrica en la CloudWatch consola.

Para ver los datos de las reglas de una ACL web

1. Inicia sesión en la CloudWatch consola AWS Management Console y ábrela en https://console.aws.amazon.com/cloudwatch/.
2. Si es necesario, cambia la región por aquella en la que se encuentran tus AWS recursos. Para CloudFront, elija la región EE. UU. Este (Virginia del Norte).
3. En el panel de navegación, en Métricas, elija Todas las métricas y, a continuación, busque en la pestaña Examinar para `AWS::WAFV2`.
4. Seleccione la casilla de verificación de la ACL web cuyos datos quiera ver.
5. Cambie la configuración aplicable:

   Estadística

   Elija el cálculo que se CloudWatch realizará con los datos.

   Intervalo de tiempo

   Elija si desea ver los datos correspondientes a la hora anterior o a las tres horas anteriores.

   Período

   Elija el intervalo entre puntos de datos del gráfico.

   Reglas

   Elija las reglas cuyos datos quiera ver.

> **Note**
>
> Si cambia el nombre de una regla y desea que el nombre de la métrica de la regla refleje el cambio, también debe actualizar el nombre de la métrica. AWS WAF no actualiza automáticamente el nombre de la métrica de una regla cuando se cambia el nombre de la regla. Puede cambiar el nombre de la métrica al editar la regla en la consola mediante el editor de reglas de JSON. También puede cambiar ambos nombres a través de las API y en cualquier lista de JSON que utilice para definir su ACL web o grupo de reglas.

Tenga en cuenta lo siguiente:

- Si asoció recientemente una ACL web a un AWS recurso, puede que tenga que esperar unos minutos para que los datos aparezcan en el gráfico y para que la métrica de la ACL web aparezca en la lista de métricas disponibles.
- Si asocia más de un recurso a una ACL web, los CloudWatch datos incluirán las solicitudes de todos ellos.
- Puede colocar el cursor sobre un punto de datos para obtener más información.
- El gráfico no se actualiza por su cuenta de forma automática. Para actualizar la pantalla, elija el icono de actualización ().

Para obtener más información sobre CloudWatch las métricas, consulteMonitorización con Amazon CloudWatch.

Paneles de información general sobre el tráfico de ACL web

En esta sección se describen los paneles de información general sobre el tráfico de ACL web de la AWS WAF consola. Después de asociar una ACL web a uno o más AWS recursos y habilitar las métricas para la ACL web, puede acceder a los resúmenes del tráfico web que evalúa la ACL web desde la pestaña de descripción general del tráfico de la ACL web de la consola. AWS WAF Los paneles incluyen resúmenes casi en tiempo real de las CloudWatch métricas de Amazon que AWS WAF recopila cuando evalúa el tráfico web de tu aplicación.

> **Note**
>
> Si no ve nada en los paneles, asegúrese de tener habilitadas las métricas para la ACL web.

La pestaña Resumen del tráfico de la ACL web contiene paneles con pestañas con las siguientes categorías de información:

- Todo el tráfico: todas las solicitudes web que evalúa la ACL web.

  El panel se centra en finalizar las acciones, pero puede ver las coincidencias con las reglas de recuento en las siguientes ubicaciones:

  - Panel de Las 10 reglas principales de este panel. Active Cambio para contar las acciones para mostrar las coincidencias de las reglas de conteo.
  - Pestaña Solicitudes muestreadas de la página de ACL web. Esta nueva pestaña incluye un gráfico de todas las coincidencias de las reglas. Para obtener más información, consulte Visualizar una muestra de solicitudes web.
- Control de bots: la web solicita que la ACL web evalúe mediante el grupo de reglas administrado de control de bots.

  Si no utiliza este grupo de reglas en su ACL web, en esta pestaña se muestran los resultados de la evaluación de una muestra de su tráfico web en función de las reglas de control de bots. Esto le da una idea del tráfico de bots que recibe su aplicación y es gratuito.

  Este grupo de reglas forma parte de las opciones inteligentes de mitigación de amenazas que AWS WAF ofrece. Para más información, consulte AWS WAF Control de bots y AWS WAF Grupo de reglas de control de bots.
- Prevención de apropiación de cuentas: la web solicita que la ACL web evalúe utilizando el grupo de reglas gestionado para la prevención de apropiación de cuentas (ATP) de AWS WAF Fraud Control. Esta pestaña solo está disponible si utiliza este grupo de reglas en su ACL web.

  Este grupo de reglas de ATP forma parte de las opciones de mitigación de amenazas inteligentes que ofrece AWS WAF . Para más información, consulte AWS WAF Control de fraudes y prevención de apropiación de cuentas (ATP) y AWS WAF Grupo de reglas de prevención de apropiación de cuentas (ATP) para el control del fraude.
- Prevención del fraude en la creación de cuentas: la web solicita que la ACL web evalúe utilizando el grupo de reglas gestionado para la prevención del AWS WAF fraude en la creación de cuentas

(ACFP) de Fraud Control. Esta pestaña solo está disponible si utiliza este grupo de reglas en su ACL web.

Este grupo de reglas de ACFP forma parte de las opciones de mitigación de amenazas inteligentes que ofrece AWS WAF . Para más información, consulte AWS WAF Control de fraude: creación de cuentas y prevención del fraude (ACFP) y AWS WAF Grupo de reglas de prevención del fraude (ACFP) para la creación de cuentas de Control de Fraude.

Los paneles se basan en las CloudWatch métricas de la ACL web y los gráficos proporcionan acceso a las métricas correspondientes. CloudWatch En el caso de los paneles de mitigación de amenazas inteligentes, como en el control de bots, las métricas utilizadas son principalmente las métricas de etiquetas.

- Para obtener una lista de las métricas que AWS WAF proporciona, consulteAWS WAF métricas y dimensiones.
- Para obtener información sobre CloudWatch las métricas, consulta la Guía del CloudWatch usuario de Amazon.

Los paneles proporcionan resúmenes de sus patrones de tráfico para las acciones de finalización y el intervalo de fechas que seleccione. Los paneles de mitigación de amenazas inteligentes incluyen solicitudes que evaluó el grupo de reglas administrado correspondiente, independientemente de si el propio grupo de reglas administrado aplicó la acción de finalización. Por ejemplo, si se selecciona Block, el panel de control Prevención de apropiación de cuentas incluye información sobre todas las solicitudes web que fueron evaluadas por el grupo de reglas administrado de la ATP y bloqueadas en algún momento durante la evaluación de la ACL web. Las solicitudes pueden bloquearse mediante el grupo de reglas administrado de la ATP, mediante una regla que se ejecute después del grupo de reglas en la ACL web o mediante la acción predeterminada de la ACL web.

Visualización de los paneles de control de una ACL web

Siga el procedimiento de esta sección para acceder a los paneles de control de la ACL web y establecer los criterios de filtrado de datos. Si asoció recientemente una ACL web a un AWS recurso, es posible que tenga que esperar unos minutos para que los datos estén disponibles en los paneles.

Los paneles de control incluyen las solicitudes de todos los recursos que ha asociado a la ACL web.

Para ver los paneles de control de Resumen del tráfico de una ACL web

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, elija ACL web y, a continuación, busque la ACL web que le interese.
3. Seleccione la ACL web. La consola le lleva a la página de la ACL web. La pestaña Resumen del tráfico está seleccionada de manera predeterminada.
4. Cambie la configuración de Filtros de datos según sea necesario.

    - Acciones de reglas de finalización: seleccione las acciones de finalización para incluirlas en los paneles de control. Los paneles resumen las métricas de las solicitudes web a las que se aplicó una de las acciones seleccionadas en la evaluación de la ACL web. Si selecciona todas las acciones disponibles, los paneles incluyen todas las solicitudes web evaluadas. Para obtener información acerca de las acciones , consulte Cómo AWS WAF gestiona las acciones de reglas y grupos de reglas en una ACL web.
    - Intervalo de tiempo: seleccione el intervalo de tiempo que desee ver en los paneles de control. Puede elegir ver un período de tiempo relativo al momento actual, por ejemplo, las últimas 3 horas o la última semana, y puede seleccionar un rango de tiempo absoluto de un calendario.
    - Zona horaria: esta configuración se aplica cuando se especifica un rango de tiempo absoluto. Puede utilizar la zona horaria local de su navegador o UTC (hora universal coordinada).

Revise la información de las pestañas que le interese. Las selecciones de filtros de datos se aplican a todos los paneles. En los paneles de gráficos, puede colocar el cursor sobre un punto de datos o un área para ver cualquier detalle adicional.

Reglas de acción Count

Puede ver la información sobre las coincidencias de las acciones de recuento en uno de estos dos lugares.

- En esta pestaña Resumen del tráfico, en el panel Todo el tráfico, encuentre el panel de Las 10 reglas principales y presione Cambiar para contar las acciones. Cuando esto está activado, el panel mostrará todas las coincidencias de reglas en lugar de las coincidencias de reglas de finalización.
- En la pestaña Solicitudes muestreadas de la ACL web, consulte un gráfico de todas las coincidencias y acciones de las reglas para el intervalo de tiempo que haya establecido en la

pestaña Resumen del tráfico. Para obtener información sobre la pestaña Solicitudes muestreadas, consulte Visualizar una muestra de solicitudes web.

CloudWatch Métricas de Amazon

En los paneles de gráficos del panel de control, puedes acceder a las CloudWatch métricas de los datos graficados. Elija la opción que se encuentra en la parte superior del panel gráfico o en el ⋮ (puntos suspensivos verticales) menú desplegable que se encuentra dentro del panel.

Actualización de los paneles

Los paneles no se actualizan automáticamente. Para actualizar la pantalla, elija el icono de actualización

.

Ejemplos de paneles de información sobre el tráfico de una ACL web

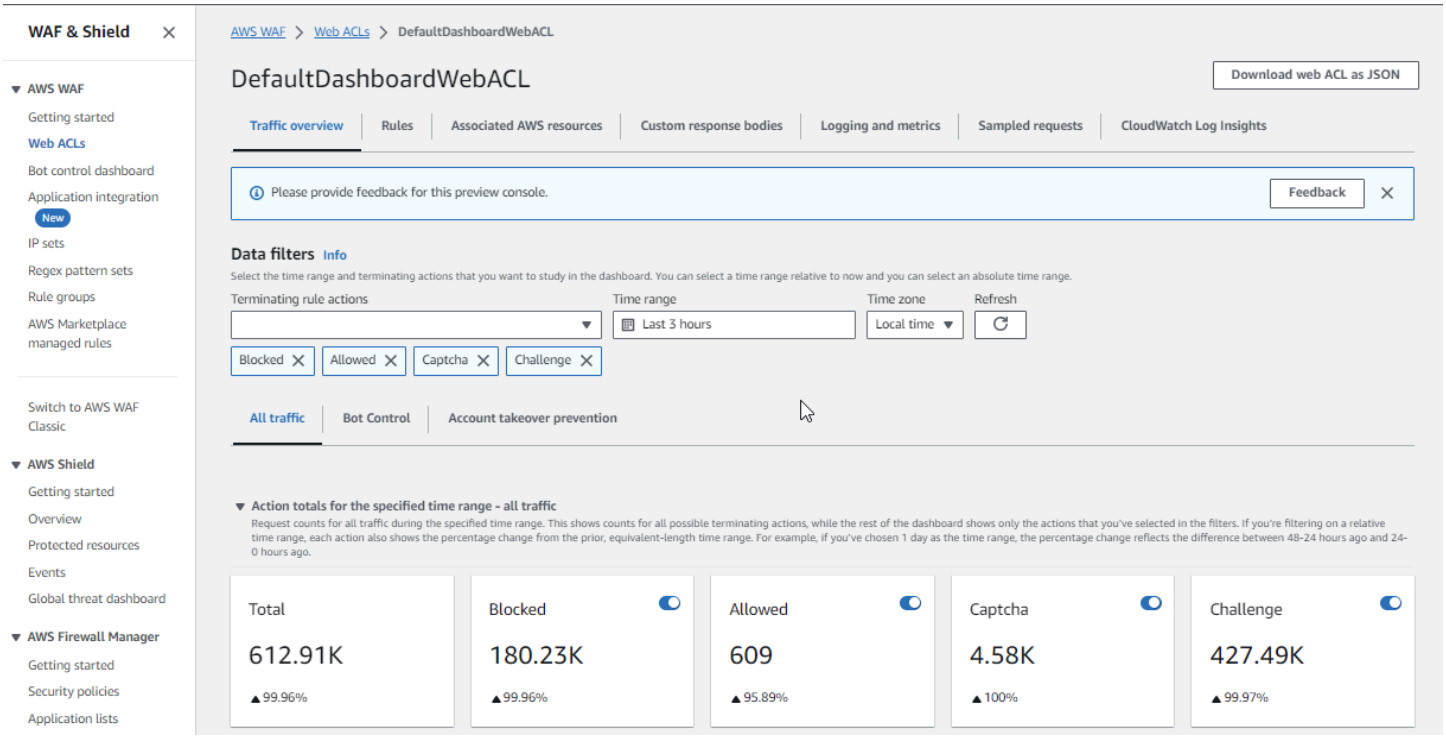
En esta sección, se muestran pantallas de ejemplo de los paneles de información general del tráfico para las ACL web.

> **Note**
>
> Si ya los utiliza AWS WAF para proteger los recursos de su aplicación, puede ver los paneles de cualquiera de sus ACL web en su página de la AWS WAF consola. Para obtener más información, consulte Visualización de los paneles de control de una ACL web.

Pantalla de ejemplo: filtros de datos y recuentos de acciones del panel de control Todo el tráfico

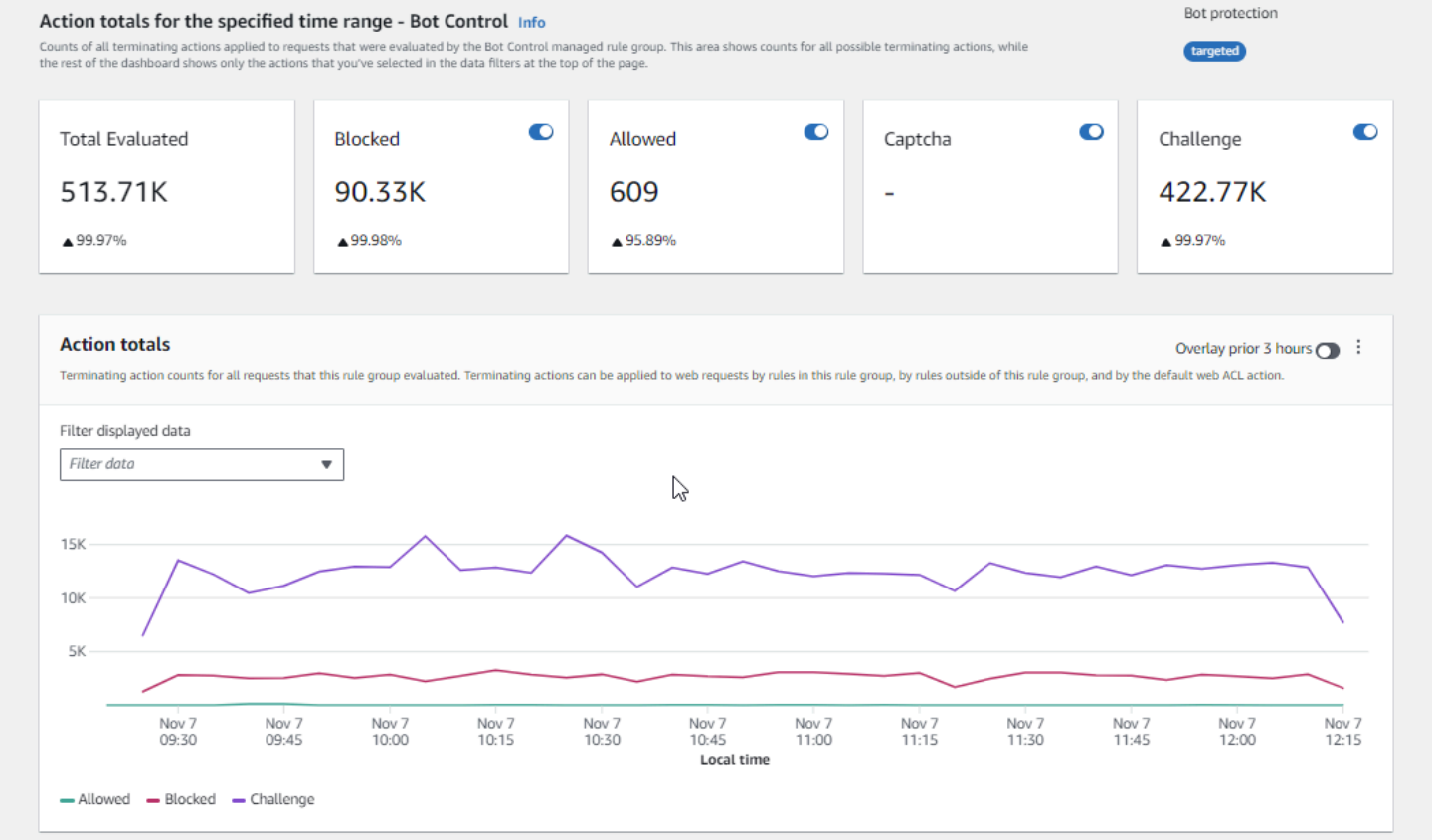
La siguiente captura de pantalla muestra la descripción general del tráfico de una ACL web con la pestaña Todo el tráfico seleccionada. Los filtros de datos están configurados en los valores predeterminados: todas las acciones de finalización durante las últimas tres horas.

En el panel de control de todo el tráfico se encuentran los totales de las distintas acciones de finalización. Cada panel muestra el recuento de solicitudes y muestra una flecha hacia arriba o hacia abajo que indica el cambio durante las tres horas anteriores.



Pantalla de ejemplo: recuentos de acciones del panel de control Control de bots

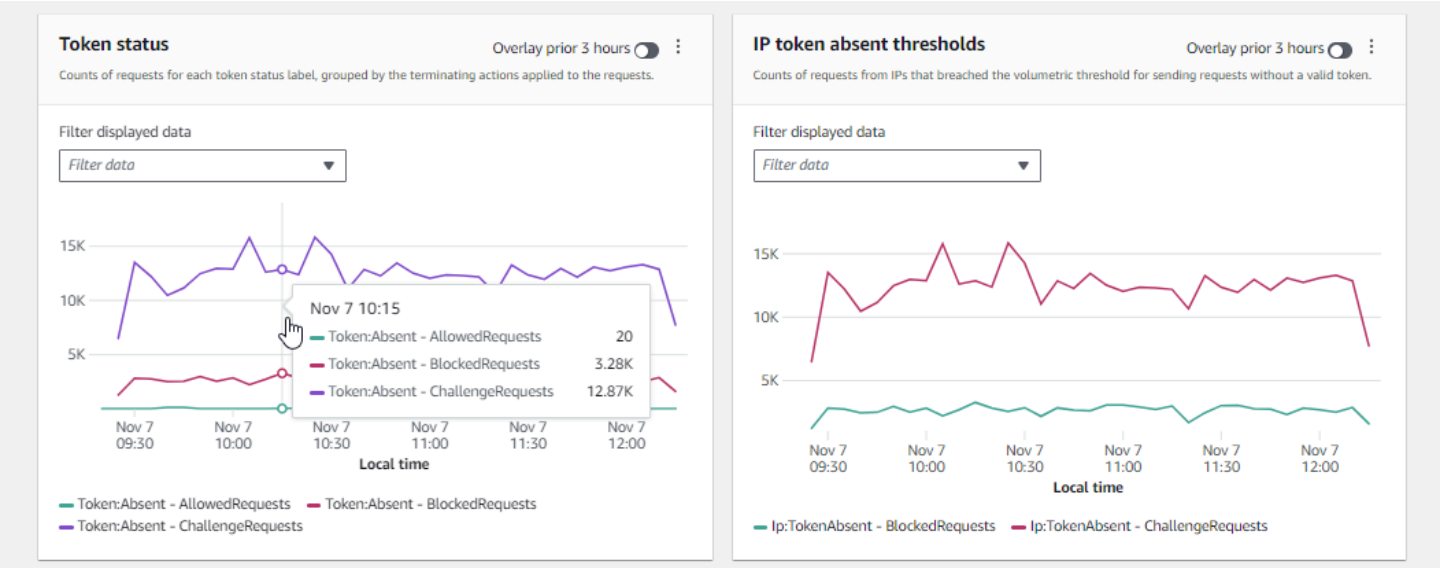
En la siguiente captura de pantalla, se muestran los recuentos de acciones del panel de control de bots. Se muestran los mismos paneles de totales para el intervalo de tiempo, pero los recuentos se refieren únicamente a las solicitudes evaluadas por el grupo de reglas de control de bots. Más abajo, en el panel Totales de acciones, puede ver los recuentos de acciones en el intervalo de tiempo especificado de tres horas. Durante este intervalo de tiempo, la acción CAPTCHA no se aplicó a ninguna de las solicitudes evaluadas por el grupo de reglas.



Pantalla de ejemplo: gráficos de resumen del estado de los tokens del panel de control Control de bots

La siguiente captura de pantalla muestra dos de los gráficos de resumen disponibles en el panel de control de bots. El panel Estado de token muestra los recuentos de las distintas etiquetas de estado del token, junto con la acción de regla que se aplicó a la solicitud. El panel Umbrales ausentes del token de IP muestra los datos de las solicitudes de las IP que estaban enviando demasiadas solicitudes sin un token.

Al pasar el ratón sobre cualquier área del gráfico, aparecen los detalles de la información disponible. En el panel Estado de token de esta captura de pantalla, el ratón pasa sobre un punto en el tiempo sin situarse sobre ninguna línea del gráfico, por lo que la consola muestra los datos de todas las líneas en ese momento.



Esta sección muestra solo algunos de los resúmenes de tráfico que se proporcionan en los paneles de información general sobre el tráfico de las ACL web. Para ver los paneles de cualquiera de sus ACL web, abra la página de la ACL web en la consola. Para obtener información acerca de cómo hacerlo, consulte las orientaciones en Visualización de los paneles de control de una ACL web.

Visualizar una muestra de solicitudes web

En esta sección se describe la pestaña de solicitudes muestreadas de ACL web de la AWS WAF consola. En esta pestaña, puede ver un gráfico de todas las coincidencias de reglas de las solicitudes web que se AWS WAF han inspeccionado. Además, si ha activado el muestreo de solicitudes para la ACL web, puede ver una vista en tabla de una muestra de las solicitudes web que se AWS WAF han inspeccionado. También puede recuperar la información de la solicitud muestreada mediante la llamada `GetSampledRequests` a la API.

La muestra de solicitudes contiene hasta 100 solicitudes que coincidieron con los criterios de una regla en la ACL web y otras 100 solicitudes de solicitudes que no coincidieron con ninguna de las reglas y que tenían aplicada la acción predeterminada de la ACL web. Las solicitudes del ejemplo vienen de todos los recursos protegidos que han recibido solicitudes de su contenido en las tres horas anteriores.

Cuando una solicitud web coincide con los criterios de una regla y la acción correspondiente a esa regla no finaliza la evaluación de la solicitud, AWS WAF continúa inspeccionando la solicitud web utilizando las reglas siguientes de la ACL web. Por este motivo, una solicitud web podría aparecer varias veces. Para obtener información sobre los comportamientos de las acciones de las reglas, consulte Acción de regla.

Para ver el gráfico de todas las reglas y las solicitudes muestreadas

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, seleccione Web ACLs (ACL web).
3. Elija el nombre de la ACL web para la que desea ver las solicitudes. La consola le lleva a la descripción de la ACL web, donde puede editarla.
4. En la pestaña Solicitudes muestreadas, puede ver lo siguiente:

   - Gráfico de todas las reglas: este gráfico muestra las reglas coincidentes y las acciones de estas para todas las evaluaciones de solicitudes web que se realizaron durante el intervalo de tiempo indicado.

     > **Note**
     >
     > El intervalo de tiempo de este gráfico se establece en la pestaña Descripción general del tráfico de la ACL web, en la sección de Filtros de datos. Para obtener más información, consulte Visualización de los paneles de control de una ACL web.

   - Tabla de solicitudes muestreadas: esta tabla muestra los datos de las solicitudes muestreadas de las últimas 3 horas. Para cada entrada, la tabla muestra los siguientes datos:

     Nombre de métrica

     El nombre de la CloudWatch métrica de la regla de la ACL web que coincidió con la solicitud. Si una solicitud web no coincide con ninguna regla de la ACL web, este valor es Predeterminado.

     > **Note**
     >
     > Si cambia el nombre de una regla y desea que el nombre de la métrica de la regla refleje el cambio, también debe actualizar el nombre de la métrica. AWS WAF no actualiza automáticamente el nombre de la métrica de una regla cuando se cambia el nombre de la regla. Puede cambiar el nombre de la métrica al editar la regla en la consola mediante el editor de reglas de JSON. También puede cambiar ambos nombres a través de las API y en cualquier lista de JSON que utilice para definir su ACL web o grupo de reglas.

IP de origen

La dirección IP desde la que se originó la solicitud o, si el espectador ha usado un proxy HTTP o un equilibrador de carga de aplicación para enviar la solicitud, la dirección IP del proxy o el equilibrador de carga de aplicación.

URI

Es la parte de una URL que identifica un recurso, por ejemplo, `/images/daily-ad.jpg`.

Regla dentro de un grupo de reglas

Si el nombre de la métrica identifica una instrucción de referencia de un grupo de reglas, identifica la regla dentro del grupo de reglas que coincidió con la solicitud.

Acción

Indica la acción de la regla correspondiente. Para obtener información sobre las acciones posibles de las reglas, consulte Acción de regla.

Tiempo

La hora a la que se AWS WAF recibió la solicitud del recurso protegido.

Para mostrar información adicional sobre los componentes de una solicitud web, elija el nombre del URI en la fila de la solicitud.

Habilitación de sus protecciones en la producción

Cuando haya terminado la fase final de pruebas y ajustes en su entorno de producción, active las protecciones en modo de producción.

> **Riesgo de tráfico de producción**
>
> Antes de implementar cambios en su ACL web para el tráfico de producción, pruébelos y ajústelos en un entorno de prueba hasta que se sienta cómodo con el posible impacto en el tráfico. Pruébelo también y ajústelo en modo recuento con su tráfico de producción antes de habilitar sus protecciones para el tráfico de producción.

> **Note**
>
> Para seguir las instrucciones de esta sección, debe comprender en general cómo crear y administrar AWS WAF protecciones, como las ACL web, las reglas y los grupos de reglas. Esta información se describe en secciones anteriores de esta guía.

Realice estos pasos primero en su entorno de prueba y, después, en producción.

Habilite sus AWS WAF protecciones en producción

1. Cambio de sus protecciones de producción

   Actualice su ACL web y cambie la configuración de producción.

   a. Eliminación de las reglas de prueba que no necesite

      Si ha agregado reglas de prueba que no necesita en producción, elimínelas. Si utiliza alguna regla de coincidencia de etiquetas para filtrar los resultados de las reglas de los grupos de reglas administrados, asegúrese de mantenerlas en su lugar.

   b. Cambio a acciones de producción

      Cambie la configuración de las acciones de sus nuevas reglas por la configuración de producción prevista.

      - Regla definida en la ACL web: edite las reglas en la ACL web y cambie sus acciones en Count a sus acciones de la producción.
      - Grupo de reglas: en la configuración de la ACL web del grupo de reglas, cambie las reglas para que utilicen sus propias acciones o déjelas con la anulación de la acción Count, en función de los resultados de sus actividades de prueba y ajuste. Si utiliza alguna regla de coincidencia de etiquetas para filtrar los resultados de las reglas de un grupos de reglas, asegúrese de mantener la anulación de dicha regla.

        Para pasar a utilizar la acción de una regla, en la configuración de la ACL web, edite la instrucción de la regla para el grupo de reglas y elimine la anulación Count de la regla. Si administra la ACL web en JSON, en la instrucción de referencia del grupo de reglas, elimine la entrada de la regla de la lista `RuleActionOverrides`.
      - ACL web: si cambió la acción predeterminada de la ACL web para sus pruebas, cámbiela a su configuración de producción.

Con esta configuración, sus nuevas protecciones administrarán el tráfico web según lo previsto.

Cuando guarde su ACL web, los recursos a los que está asociada utilizarán su configuración de producción.

2. Monitorización y ajuste

   Para asegurarse de que las solicitudes web se gestionen como desea, monitorice de cerca el tráfico después de activar la nueva funcionalidad. Supervisará las métricas y los registros de monitorización de las acciones de reglas de producción en lugar de las acciones de recuento que estaba monitorizando durante el trabajo de ajuste. Siga monitorizando y ajustando el comportamiento según sea necesario para adaptarlo a los cambios en el tráfico web.

Cómo AWS WAF funciona con las CloudFront funciones de Amazon

Al crear una ACL web, puede especificar una o más CloudFront distribuciones que desee AWS WAF inspeccionar. AWS WAF comienza a inspeccionar y gestionar las solicitudes web de esas distribuciones en función de los criterios que usted identifique en la ACL web. CloudFront proporciona algunas funciones que mejoran la AWS WAF funcionalidad. En este capítulo se describen algunas formas que se pueden configurar CloudFront para mejorar CloudFront el AWS WAF funcionamiento conjunto.

Temas

- Utilización AWS WAF con páginas de error CloudFront personalizadas
- AWS WAF CloudFrontUtilízalo con aplicaciones que se ejecutan en tu propio servidor HTTP
- Elegir los métodos HTTP que CloudFront respondan a

Utilización AWS WAF con páginas de error CloudFront personalizadas

De forma predeterminada, cuando AWS WAF bloquea una solicitud web en función de los criterios que especifiques CloudFront, devuelve el código `403 (Forbidden)` de estado HTTP y lo CloudFront devuelve al espectador. El visor muestra un breve mensaje predeterminado con formato elemental similar al que se muestra a continuación:

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

Puede anular este comportamiento en las reglas de ACL AWS WAF web definiendo respuestas personalizadas. Para obtener más información sobre cómo personalizar el comportamiento de respuesta mediante AWS WAF reglas, consulte. Respuestas personalizadas para las acciones Block

> **Note**
>
> Las respuestas que personalice mediante AWS WAF reglas tienen prioridad sobre cualquier especificación de respuesta que defina en las páginas de error CloudFront personalizadas.

Si prefieres mostrar un mensaje de error personalizado CloudFront, posiblemente con el mismo formato que el resto del sitio web, puedes configurarlo para que devuelva CloudFront al espectador un objeto (por ejemplo, un archivo HTML) que contenga tu mensaje de error personalizado.

> **Note**
>
> CloudFront no puedes distinguir entre un código de estado HTTP 403 que devuelve tu origen y otro que devuelve AWS WAF cuando se bloquea una solicitud. Esto significa que no puede devolver diferentes páginas de error personalizadas en función de las diferentes causas de un código de estado HTTP 403.

Para obtener más información sobre las páginas de error CloudFront personalizadas, consulta Generar respuestas de error personalizadas en la Guía para CloudFront desarrolladores de Amazon.

AWS WAF CloudFrontUtilízalo con aplicaciones que se ejecutan en tu propio servidor HTTP

Cuando lo usas AWS WAF con CloudFront, puedes proteger tus aplicaciones que se ejecutan en cualquier servidor web HTTP, ya sea un servidor web que se ejecute en Amazon Elastic Compute Cloud (Amazon EC2) o un servidor web que administres de forma privada. También puede configurarlo CloudFront para que requiera HTTPS entre CloudFront y su propio servidor web, así como entre los espectadores y. CloudFront

Requiere HTTPS entre CloudFront y su propio servidor web

Si necesitas HTTPS entre tu servidor web CloudFront y tu propio servidor web, puedes usar la función de origen CloudFront personalizado y configurar la política de protocolo de origen y los ajustes del nombre de dominio de origen para orígenes específicos. En tu CloudFront configuración, puedes especificar el nombre DNS del servidor junto con el puerto y el protocolo que quieres usar CloudFront para recuperar objetos de tu origen. También debe asegurarse de que el certificado SSL/TLS del servidor de origen personalizado coincide con el nombre de dominio de origen que ha configurado. Si utiliza su propio servidor web HTTP fuera de AWS, debe utilizar un certificado firmado por una entidad emisora de certificados (CA) externa de confianza, por ejemplo, Comodo o Symantec DigiCert. Para obtener más información sobre cómo se requiere HTTPS para la comunicación entre CloudFront y su propio servidor web, consulte el tema Requerir HTTPS para la comunicación entre CloudFront y su origen personalizado en la Guía para CloudFront desarrolladores de Amazon.

Requerir HTTPS entre un espectador y CloudFront

Para requerir HTTPS entre los espectadores y CloudFront, puede cambiar la política de protocolo de visualización para uno o más comportamientos de caché en su CloudFront distribución. Para obtener más información sobre el uso de HTTPS entre espectadores CloudFront, consulte el tema Exigir HTTPS para la comunicación entre espectadores y CloudFront en la Guía para CloudFront desarrolladores de Amazon. También puedes traer tu propio certificado SSL para que los espectadores puedan conectarse a tu CloudFront distribución a través de HTTPS con tu propio nombre de dominio, por ejemplo, https://www.mysite.com. Para obtener más información, consulte el tema Configuración de nombres de dominio alternativos y HTTPS en la Guía para CloudFront desarrolladores de Amazon.

Elegir los métodos HTTP que CloudFront respondan a

Cuando creas una distribución CloudFront web de Amazon, eliges los métodos HTTP que quieres CloudFront procesar y reenviar a tu origen. Puede elegir entre las siguientes opciones:

- **`GET`**, **`HEAD`** — CloudFront Solo puedes usarlos para obtener objetos de tu origen o para obtener encabezados de objetos.
- **`GET`**,**`HEAD`**, **`OPTIONS`** — CloudFront Solo puedes usarlo para obtener objetos de tu origen, obtener encabezados de objetos o recuperar una lista de las opciones que admite tu servidor de origen.
- **`GET`**,**`HEAD`**,**`OPTIONS`**,**`PUT`**,, **`POSTPATCH`**, **`DELETE`** — Se puede utilizar CloudFront para obtener, añadir, actualizar y eliminar objetos, así como para obtener encabezados de objetos. Además, puede realizar otras operaciones de `POST` como enviar datos desde un formulario web.

También puede usar sentencias de reglas de coincidencia de AWS WAF bytes para permitir o bloquear las solicitudes según el método HTTP, tal y como se describe enInstrucción de regla de coincidencia de cadenas. Si desea utilizar una combinación de métodos CloudFront compatibles, como `GET` y`HEAD`, no necesita configurarla AWS WAF para bloquear las solicitudes que utilizan los otros métodos. Si desea permitir una combinación de métodos que CloudFront no sea compatible, por ejemplo, y `GET HEADPOST`, puede configurarla para que responda CloudFront a todos los métodos y, a continuación, utilizarla AWS WAF para bloquear las solicitudes que utilizan otros métodos.

Para obtener más información sobre cómo elegir los métodos CloudFront adecuados, consulte Métodos HTTP permitidos en el tema Valores que se especifican al crear o actualizar una distribución web de la Guía para CloudFront desarrolladores de Amazon.

Seguridad en el uso del AWS WAF servicio

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

> **Note**
>
> Esta sección proporciona una guía AWS de seguridad estándar para el uso del AWS WAF servicio y sus AWS recursos, como las ACL AWS WAF web y los grupos de reglas. Para obtener información sobre cómo proteger sus AWS recursos mediante el uso AWS WAF, consulte el resto de la AWS WAF guía.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad aplicables AWS WAF, consulte los AWS servicios incluidos en el ámbito de aplicación por programa de conformidad.

- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS WAF. Los siguientes temas muestran cómo configurarlo AWS WAF para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus AWS WAF recursos.

Temas

Protección de datos en AWS WAF

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS WAF. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice autenticación multifactor (MFA) en cada cuenta.

- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja AWS WAF o Servicios de AWS utiliza la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

AWS WAF Las entidades (como las ACL web, los grupos de reglas y los conjuntos de IP) se cifran en reposo, excepto en determinadas regiones en las que el cifrado no está disponible, como China (Pekín) y China (Ningxia). Para cada región se utilizan claves de cifrado únicas.

Eliminación de recursos de AWS WAF

Puede eliminar los recursos que creó en AWS WAF. Consulte las directrices para cada tipo de recurso en las siguientes secciones.

- Eliminación de una ACL web
- Eliminar un grupo de reglas
- Eliminar un conjunto de IP
- Eliminar un conjunto de patrones de expresiones regex

Administración de identidad y acceso para AWS WAF

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS WAF La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo en el que se realice. AWS WAF

Usuario del servicio: si utiliza el AWS WAF servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más AWS WAF funciones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en AWS WAF, consulte Solución de problemas AWS WAF de identidad y acceso.

Administrador de servicios: si estás a cargo de AWS WAF los recursos de tu empresa, probablemente tengas acceso total a ellos AWS WAF. Su trabajo consiste en determinar a qué AWS WAF funciones y recursos deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM AWS WAF, consulteCómo AWS WAF funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a AWS. Para ver ejemplos de políticas AWS WAF basadas en la identidad que puede utilizar en IAM, consulte. Ejemplos de políticas basadas en identidades de AWS WAF

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS Single Sign-On y Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la

contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS Single Sign-On. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS Single Sign-On.
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, en algunos casos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute

aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.

- Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
- Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifique el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations

AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.

- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo AWS WAF funciona con IAM

Antes de utilizar IAM para gestionar el acceso AWS WAF, infórmese sobre las funciones de IAM disponibles para su uso. AWS WAF

Funciones de IAM que puede utilizar con AWS WAF

Característica de IAM	AWS WAF soporte
Políticas basadas en identidades	Sí
Políticas basadas en recursos	Sí
Acciones de políticas	Sí
Recursos de políticas	Sí

Característica de IAM	AWS WAF soporte
Claves de condición de política (específicas del servicio)	Sí
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo AWS WAF funcionan otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para AWS WAF

Compatibilidad con las políticas basadas en identidades	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Para ver ejemplos de políticas AWS WAF basadas en la identidad, consulte. Ejemplos de políticas basadas en identidades de AWS WAF

Políticas basadas en recursos incluidas AWS WAF

Compatibilidad con las políticas basadas en recursos	Sí

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

AWS WAF utiliza políticas basadas en recursos para permitir el uso compartido de grupos de reglas entre cuentas. Para compartir un grupo de reglas de su propiedad con otra AWS cuenta, debe proporcionar la configuración de políticas basada en recursos a la llamada a la AWS WAF API `PutPermissionPolicy` o a una llamada de CLI o SDK equivalente. Para obtener información adicional, incluidos ejemplos y enlaces a la documentación de los demás idiomas disponibles, consulta la referencia de PutPermissionPolicyla AWS WAF API. Esta funcionalidad no está disponible a través de otros medios, como la consola o. AWS CloudFormation

Acciones políticas para AWS WAF

Admite acciones de política	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de AWS WAF acciones y permisos para cada una de ellas, consulta las acciones definidas por la AWS WAF versión 2 en la Referencia de autorización de servicios.

Las acciones políticas AWS WAF utilizan el siguiente prefijo antes de la acción:

```
wafv2
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "wafv2:action1",
      "wafv2:action2"
         ]
```

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones AWS WAF que comiencen por`List`, incluya la siguiente acción:

```
"Action": "wafv2:List*"
```

Para ver ejemplos de políticas AWS WAF basadas en la identidad, consulte. Ejemplos de políticas basadas en identidades de AWS WAF

Acciones que requieren configuraciones de permisos adicionales

Algunas acciones requieren permisos que no se pueden describir completamente en las acciones definidas por la AWS WAF versión 2 de la Referencia de autorización de servicios. En esta sección, se proporciona información adicional sobre los permisos.

Temas

- Permisos para AssociateWebACL
- Permisos para DisassociateWebACL
- Permisos para GetWebACLForResource
- Permisos para ListResourcesForWebACL

Permisos para **`AssociateWebACL`**

En esta sección, se enumeran los permisos necesarios para asociar una ACL web a un recurso mediante la acción `AssociateWebACL` de AWS WAF .

Para CloudFront las distribuciones de Amazon, usa la acción en lugar de esta CloudFront acción`UpdateDistribution`. Para obtener más información, consulta UpdateDistributionla referencia de la CloudFront API de Amazon.

API de REST de Amazon API Gateway

Requiere permiso para llamar a API Gateway `SetWebACL` en el tipo de recurso de API REST y para llamar AWS WAF `AssociateWebACL` a una ACL web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
```

```
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}
```

Equilibrador de carga de aplicación

Requiere permiso para realizar una `elasticloadbalancing:SetWebACL` acción en el tipo de recurso Application Load Balancer y para llamar a una AWS WAF `AssociateWebACL` ACL web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:SetWebACL"
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

AWS AppSync API GraphQL

Requiere permiso para invocar AWS AppSync `SetWebACL` el tipo de recurso de la API GraphQL y para llamar a una AWS WAF `AssociateWebACL` ACL web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
```

```
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Grupo de usuarios de Amazon Cognito

Requiere permiso para llamar a la `AssociateWebACL` acción de Amazon Cognito en el tipo de recurso del grupo de usuarios y para llamar a una AWS WAF `AssociateWebACL` ACL web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner servicio

Requiere permiso para llamar a la `AssociateWebACL` acción de App Runner en el tipo de recurso de servicio de App Runner y para llamar AWS WAF `AssociateWebACL` a una ACL web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:AssociateWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS Instancia de acceso verificado

Requiere permiso para ejecutar la `ec2:AssociateVerifiedAccessInstanceWebAcl` acción en el tipo de recurso de la instancia de acceso verificado y para llamar AWS WAF `AssociateWebACL` a una ACL web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
```

```
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:AssociateVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

Permisos para **`DisassociateWebACL`**

En esta sección se enumeran los permisos necesarios para desasociar una ACL web de un recurso mediante la AWS WAF acción`DisassociateWebACL`.

Para CloudFront las distribuciones de Amazon, en lugar de esta acción, usa la CloudFront acción `UpdateDistribution` con un ID de ACL web vacío. Para obtener más información, consulta UpdateDistributionla referencia de la CloudFront API de Amazon.

API de REST de Amazon API Gateway

Requiere permiso para llamar a API Gateway `SetWebACL` en el tipo de recurso de API de REST. No requiere permiso para llamar AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}
```

Equilibrador de carga de aplicación

Requiere permiso para llamar a la acción `elasticloadbalancing:SetWebACL` en el tipo de recurso equilibrador de carga de aplicación. No requiere permiso para llamar AWS WAF `DisassociateWebACL`.

```
{
```

```
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:SetWebACL"
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

AWS AppSync API GraphQL

Requiere permiso para llamar al tipo AWS AppSync `SetWebACL` de recurso de la API GraphQL. No requiere permiso para llamar AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Grupo de usuarios de Amazon Cognito

Requiere permiso para ejecutar la `DisassociateWebACL` acción de Amazon Cognito en el tipo de recurso del grupo de usuarios y para realizar la llamada. AWS WAF `DisassociateWebACL`

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:DisassociateWebACL"
    ],
```

```
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner servicio

Requiere permiso para ejecutar la `DisassociateWebACL` acción de App Runner en el tipo de recurso de servicio de App Runner y realizar la llamada AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:DisassociateWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS Instancia de acceso verificado

Requiere permiso para ejecutar la `ec2:DisassociateVerifiedAccessInstanceWebAcl` acción en el tipo de recurso de la instancia de Verified Access y realizar la llamada AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
```

```
    "Action": [
        "ec2:DisassociateVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

Permisos para **`GetWebACLForResource`**

En esta sección se enumeran los permisos necesarios para obtener la ACL web para un recurso protegido mediante la AWS WAF acción de `GetWebACLForResource`.

Para CloudFront las distribuciones de Amazon, usa la acción en lugar de esta CloudFront acción`GetDistributionConfig`. Para obtener más información, consulta GetDistributionConfigla referencia de la CloudFront API de Amazon.

> **Note**
>
> `GetWebACLForResource` requiere el permiso para llamar a `GetWebACL`. En este contexto, `GetWebACL` solo se AWS WAF usa para verificar que su cuenta tiene el permiso que necesita para acceder a la ACL web que `GetWebACLForResource` devuelve. Cuando llames`GetWebACLForResource`, es posible que aparezca un error que indique que tu cuenta no está autorizada a operar con `wafv2:GetWebACL` el recurso. AWS WAF no añade este tipo de error al historial de AWS CloudTrail eventos.

API REST, Application Load Balancer y AWS AppSync GraphQL de Amazon API Gateway

Se requiere permiso para realizar llamadas AWS WAF `GetWebACLForResource` y `GetWebACL` para una ACL web.

```
{
    "Sid": "GetWebACLForResource",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
```

```
    ]
}
```

Grupo de usuarios de Amazon Cognito

Requiere permiso para llamar a la `GetWebACLForResource` acción de Amazon Cognito en el tipo de recurso del grupo de usuarios y para llamar AWS WAF `GetWebACLForResource` a y. `GetWebACL`

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:GetWebACLForResource"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner servicio

Requiere permiso para llamar a la `DescribeWebAclForService` acción de App Runner en el tipo de recurso de servicio de App Runner y para llamar a AWS WAF `GetWebACLForResource` y`GetWebACL`.

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
```

```
            "wafv2:GetWebACL"
        ],
        "Resource": [
            "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
        ]
    },
    {
        "Sid": "GetWebACLForResource2",
        "Effect": "Allow",
        "Action": [
            "apprunner:DescribeWebAclForService"
        ],
        "Resource": [
            "arn:aws:apprunner:*:account-id:service/*/*"
        ]
    }
```

AWS Instancia de acceso verificado

Requiere permiso para ejecutar la `ec2:GetVerifiedAccessInstanceWebAcl` acción en el tipo de recurso de la instancia de acceso verificado y para llamar a AWS WAF `GetWebACLForResource` y`GetWebACL`.

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "ec2:GetVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
```

```
}
```

Permisos para **`ListResourcesForWebACL`**

En esta sección, se enumeran los permisos necesarios para recuperar la lista de recursos protegidos para una ACL web mediante la acción `ListResourcesForWebACL` de AWS WAF .

Para CloudFront las distribuciones de Amazon, usa la acción en lugar de esta CloudFront acción`ListDistributionsByWebACLId`. Para obtener más información, consulta ListDistributionsByWebaclID en la referencia de CloudFront API de Amazon.

API REST, Application Load Balancer y AWS AppSync GraphQL de Amazon API Gateway

Se requiere permiso AWS WAF `ListResourcesForWebACL` para solicitar una ACL web.

```
{
    "Sid": "ListResourcesForWebACL",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

Grupo de usuarios de Amazon Cognito

Requiere permiso para llamar a la acción `ListResourcesForWebACL` de Amazon Cognito en el tipo de recurso de grupo de usuarios y para llamar a `ListResourcesForWebACL` de AWS WAF .

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
```

```
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner servicio

Requiere permiso para ejecutar la `ListAssociatedServicesForWebAcl` acción de App Runner en el tipo de recurso de servicio de App Runner y realizar la llamada AWS WAF `ListResourcesForWebACL`.

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:ListAssociatedServicesForWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS Instancia de acceso verificado

Requiere permiso para llamar a la acción `ec2:DescribeVerifiedAccessInstanceWebAclAssociations` en el tipo de recurso de instancia de acceso verificado y llamar a `ListResourcesForWebACL` de AWS WAF .

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

Recursos de políticas para AWS WAF

Admite recursos de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver la lista de tipos de AWS WAF recursos y sus ARN, consulte los recursos definidos por la AWS WAF versión 2 en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS WAF V2. Para permitir o denegar el acceso a un subconjunto de AWS WAF recursos, incluya el ARN del recurso en el elemento de `resource` la política.

Los ARN de los AWS WAF `wafv2` recursos tienen el siguiente formato:

```
arn:partition:wafv2:region:account-id:scope/resource-type/resource-name/resource-id
```

Para obtener información general acerca de las especificaciones de ARN, consulte Nombres de recursos de Amazon (ARN) en la Referencia general de Amazon Web Services.

A continuación, se enumeran los requisitos específicos de los ARN de los recursos de `wafv2`:

- *`región`*: En el caso de AWS WAF los recursos que utilizas para proteger CloudFront las distribuciones de Amazon, establécela en. `us-east-1` De lo contrario, establézcalo en la región que esté utilizando con sus recursos regionales protegidos.
- *`alcance`*: defina el ámbito `global` para usarlo con una CloudFront distribución de Amazon o `regional` para usarlo con cualquiera de los recursos regionales AWS WAF compatibles. Los recursos regionales son una API REST de Amazon API Gateway, un Application Load Balancer, una API AWS AppSync GraphQL, un grupo de usuarios de Amazon Cognito, un AWS App Runner servicio y una instancia de Verified Access. AWS
- *`Tipo de recurso`*: especifique uno de los siguientes valores: `webacl`, `rulegroup`, `ipset`, `regexpatternset` o `managedruleset`.
- *`Nombre-recurso`*: especifique el nombre que asignó al recurso de AWS WAF o especifique un comodín (`*`) para indicar todos los recursos que cumplen las demás especificaciones del ARN. Debe especificar el nombre y el identificador del recurso, o especificar un comodín para ambos.
- *`resource-id`*: especifique el ID del recurso de AWS WAF o especifique un comodín (`*`) para indicar todos los recursos que cumplen las demás especificaciones del ARN. Debe especificar el nombre y el identificador del recurso, o especificar un comodín para ambos.

Por ejemplo, el siguiente ARN especifica todas las ACL web con ámbito regional para la cuenta `111122223333` en la región `us-west-1`:

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

El siguiente ARN especifica el grupo de reglas denominado `MyIPManagementRuleGroup` con un alcance global para la cuenta `111122223333` en la región `us-east-1`:

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

Para ver ejemplos de políticas basadas en la AWS WAF identidad, consulte. Ejemplos de políticas basadas en identidades de AWS WAF

Claves de condición de la política para AWS WAF

Admite claves de condición de políticas específicas del servicio	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación lógica `AND`. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Además, AWS WAF admite las siguientes claves de condición que puede utilizar para proporcionar un filtrado detallado a sus políticas de IAM:

- wafv2: LogDestinationResource

  Esta clave de condición toma una especificación de Amazon Resource Name (ARN) para el destino del registro. Este es el ARN que proporciona para el destino del registro cuando utiliza la llamada a la API REST. `PutLoggingConfiguration`

  Puede especificar un ARN de forma explícita y puede especificar el filtrado del ARN. El siguiente ejemplo especifica el filtrado de los ARN de bucket de Amazon S3 que tienen una ubicación y un prefijo específicos.

  ```
  "Condition": { "ArnLike": { "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-suffix/custom-prefix/*" } }
  ```

- wafv2: LogScope

  Esta clave de condición define el origen de la configuración de registro en una cadena. Actualmente, siempre tiene el valor predeterminado de`Customer`, lo que indica que el destino del registro es de su propiedad y está gestionado por usted.

Para ver una lista de claves de AWS WAF condición, consulte las claves de condición de la AWS WAF versión 2 en la Referencia de autorización del servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por la AWS WAF V2.

Para ver ejemplos de políticas AWS WAF basadas en la identidad, consulte. Ejemplos de políticas basadas en identidades de AWS WAF

ACL en AWS WAF

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con AWS WAF

Admite ABAC (etiquetas en las políticas)	Parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Utilizar credenciales temporales con AWS WAF

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más

información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Reenvíe las sesiones de acceso para el servicio AWS WAF

Admite Forward access sessions (FAS)	Sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre las políticas a la hora de realizar solicitudes de FAS, consulte Forward access sessions.

Roles de servicio para AWS WAF

Compatible con roles de servicio	Sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio puede interrumpir AWS WAF la funcionalidad. Edite las funciones de servicio solo cuando se AWS WAF proporcionen instrucciones para hacerlo.

Funciones vinculadas al servicio para AWS WAF

Compatible con roles vinculados al servicio	Sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre la creación o la administración de funciones AWS WAF vinculadas al servicio, consulte. Uso de roles vinculados a servicios para AWS WAF

Ejemplos de políticas basadas en identidades de AWS WAF

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de AWS WAF . Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles, y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por cada uno de los tipos de recursos AWS WAF, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de la AWS WAF versión 2 en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Mediante la consola de AWS WAF
- Cómo permitir a los usuarios consultar sus propios permisos
- Otorgue acceso de solo lectura a, y AWS WAF CloudFront CloudWatch
- Conceda acceso completo a AWS WAF CloudFront, y CloudWatch
- Conceda acceso a una sola Cuenta de AWS

- Concesión de acceso a una única ACL web
- Concesión de acceso a la CLI a una ACL web y a un grupo de reglas

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear AWS WAF recursos de tu cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía del usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Mediante la consola de AWS WAF

Para acceder a la AWS WAF consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los AWS WAF recursos de su cuenta Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan usar la AWS WAF consola, adjunte también al menos la política AWS WAF `AWSWAFConsoleReadOnlyAccess` AWS administrada a las entidades. Para obtener información sobre esta política administrada, consulte AWS política gestionada: AWSWAFConsoleReadOnlyAccess. Para obtener más información sobre cómo agregar una política administrada a un usuario, consulte Agregar permisos a un usuario en la Guía del usuario de IAM.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Otorgue acceso de solo lectura a, y AWS WAF CloudFront CloudWatch

La siguiente política otorga a los usuarios acceso de solo lectura a AWS WAF los recursos, a las distribuciones CloudFront web de Amazon y a las métricas de Amazon. CloudWatch Resulta útil para los usuarios que necesitan permiso para ver la configuración de AWS WAF las condiciones, reglas y ACL web para ver qué distribución está asociada a una ACL web y para monitorizar las métricas y una muestra de solicitudes en ellas. CloudWatch Estos usuarios no pueden crear, actualizar ni eliminar recursos de AWS WAF .

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Action": [
            "wafv2:Get*",
```

```
            "wafv2:List*",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Effect": "Allow",
         "Resource": "*"
      }
   ]
}
```

Conceda acceso completo a AWS WAF CloudFront, y CloudWatch

La siguiente política permite a los usuarios realizar cualquier AWS WAF operación, realizar cualquier operación en distribuciones CloudFront web y monitorear las métricas y una muestra de solicitudes en CloudWatch ellas. Es útil para los usuarios que son AWS WAF administradores.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
            "wafv2:*",
            "cloudfront:CreateDistribution",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:UpdateDistribution",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudfront:DeleteDistribution",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Effect": "Allow",
         "Resource": "*"
      }
   ]
}
```

Recomendamos encarecidamente que configure la autenticación multifactor (MFA) para los usuarios que tienen permisos administrativos. Para obtener más información, consulte Uso de la autenticación multifactor (MFA) en dispositivos con AWS en la Guía del usuario de IAM.

Conceda acceso a una sola Cuenta de AWS

Esta política concede los siguientes permisos a la cuenta 444455556666:

- Acceso total a todas AWS WAF las operaciones y recursos.
- Lea y actualice el acceso a todas CloudFront las distribuciones, lo que le permite asociar las ACL web y CloudFront las distribuciones.
- Acceso de lectura a todas CloudWatch las métricas y estadísticas métricas para poder ver CloudWatch los datos y una muestra de las solicitudes en la consola. AWS WAF

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "wafv2:*"
         ],
         "Resource": [
            "arn:aws:wafv2:us-east-1:444455556666:*"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudfront:UpdateDistribution",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Resource": [
            "*"
         ]
```

```
      }
   ]
}
```

Concesión de acceso a una única ACL web

La siguiente política permite a los usuarios realizar cualquier AWS WAF operación a través de la consola en una ACL web específica de la cuenta444455556666.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:*"
            ],
            "Resource": [
                "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
            ]
        },
        {
            "Sid": "consoleAccess",
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs",
                "ec2:DescribeRegions"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Concesión de acceso a la CLI a una ACL web y a un grupo de reglas

La siguiente política permite a los usuarios realizar cualquier AWS WAF operación a través de la CLI en una ACL web específica y en un grupo de reglas específico de la cuenta444455556666.

```
{
```

```
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "wafv2:*"
         ],
         "Resource": [
        "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
        "arn:aws:wafv2:us-east-1:444455556666:regional/rulegroup/
test123rulegroup/555555555-6666-1234-abcd-00d11example"
         ]
      }
   ]
}
```

La siguiente política permite a los usuarios realizar cualquier AWS WAF operación a través de la consola en una ACL web específica de la cuenta444455556666.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:*"
            ],
            "Resource": [
                "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
            ]
        },
        {
            "Sid": "consoleAccess",
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs",
                "ec2:DescribeRegions"
            ],
            "Resource": [
                "*"
            ]
```

```
        }
    ]
}
```

AWS políticas gestionadas para AWS WAF

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSWAFReadOnlyAccess

Esta política otorga permisos de solo lectura que permiten a los usuarios acceder a AWS WAF recursos y recursos para servicios integrados, como Amazon, Amazon CloudFront API Gateway, Application Load Balancer, AWS AppSync Amazon Cognito y Verified Access. AWS App Runner AWS Puede adjuntar esta política a sus identidades de IAM. AWS WAF también vincula esta política a un rol de servicio que le permite AWS WAF realizar acciones en su nombre.

Para obtener más información sobre esta política, consulte AWSWAFReadOnlyAccessen la consola de IAM.

AWS política gestionada: AWSWAFFullAccess

Esta política otorga acceso total a AWS WAF los recursos y recursos de los servicios integrados, como Amazon CloudFront, Amazon API Gateway, Application Load Balancer AWS AppSync, Amazon Cognito y Verified AWS App Runner Access. AWS Puede adjuntar esta política a sus

identidades de IAM. AWS WAF también vincula esta política a un rol de servicio que le permite AWS WAF realizar acciones en su nombre.

Para obtener más información sobre esta política, consulte AWSWAFFullAccessen la consola de IAM.

AWS política gestionada: AWSWAFConsoleReadOnlyAccess

Esta política concede permisos de solo lectura a la AWS WAF consola, que incluyen recursos para AWS WAF y para servicios integrados, como Amazon, Amazon API Gateway CloudFront, Application Load Balancer, AWS AppSync Amazon Cognito y Verified Access AWS App Runner. AWS Puede adjuntar esta política a sus identidades de IAM. AWS WAF también vincula esta política a un rol de servicio que le permite AWS WAF realizar acciones en su nombre.

Para obtener más información sobre esta política, consulte AWSWAFConsoleReadOnlyAccessen la consola de IAM.

AWS política gestionada: AWSWAFConsoleFullAccess

Esta política otorga acceso total a la AWS WAF consola, que incluye recursos para AWS WAF y para servicios integrados, como Amazon CloudFront, Amazon API Gateway, Application Load Balancer AWS AppSync, Amazon Cognito y Verified AWS App Runner Access. AWS Puede adjuntar esta política a sus identidades de IAM. AWS WAF también vincula esta política a un rol de servicio que le permite AWS WAF realizar acciones en su nombre.

Para obtener más información sobre esta política, consulte AWSWAFConsoleFullAccessen la consola de IAM.

AWS WAF actualizaciones de las políticas AWS gestionadas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas AWS WAF desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del AWS WAF documento enHistorial de documentos.

Política	Descripción del cambio	Date
`AWSWAFFullAccess`	Permisos ampliados para agregar instancias de acceso	-17 de junio de 2023

Política	Descripción del cambio	Date
Esta política le permite AWS WAF administrar AWS los recursos en su nombre en los servicios integrados AWS WAF y dentro de ellos. Detalles en la consola de IAM: AWSWAFFullAccess.	AWS verificado a los tipos de recursos con AWS WAF los que puede protegerse.	
`AWSWAFReadOnlyAccess` Esta política permite administrar AWS WAF los AWS recursos en su nombre en los servicios integrados AWS WAF y dentro de ellos. Detalles en la consola de IAM: AWSWAFReadOnlyAccess.	Permisos ampliados para agregar instancias de acceso AWS verificado a los tipos de recursos con AWS WAF los que puede protegerse.	-17 de junio de 2023
`AWSWAFConsoleFullAccess` Esta política permite AWS WAF administrar los recursos de la AWS consola y otros AWS recursos en su nombre en los servicios integrados AWS WAF y dentro de ellos. Detalles en la consola de IAM: AWSWAFConsoleFullAccess.	Permisos ampliados para agregar instancias de acceso AWS verificado a los tipos de recursos con AWS WAF los que puede protegerse.	-17 de junio de 2023

Política	Descripción del cambio	Date
`AWSWAFConsoleReadOnlyAccess` Esta política permite AWS WAF administrar los recursos de la AWS consola y otros AWS recursos en su nombre en los servicios integrados AWS WAF y dentro de ellos. Detalles en la consola de IAM: AWSWAFConsoleReadOnlyAccess.	Permisos ampliados para agregar instancias de acceso AWS verificado a los tipos de recursos con AWS WAF los que puede protegerse.	-17 de junio de 2023
`AWSWAFFullAccess` Esta política permite administrar AWS WAF los AWS recursos en su nombre en los servicios integrados AWS WAF y dentro de ellos. Detalles en la consola de IAM: AWSWAFFullAccess.	Permisos ampliados para corregir la configuración de acceso a los AWS App Runner servicios.	06-06-2020
`AWSWAFReadOnlyAccess` Esta política le permite administrar AWS WAF los AWS recursos en su nombre en AWS WAF los servicios integrados y dentro de ellos. Detalles en la consola de IAM: AWSWAFReadOnlyAccess.	Permisos ampliados para corregir la configuración de acceso a los AWS App Runner servicios.	06-06-2020

Política	Descripción del cambio	Date
`AWSWAFConsoleFullAccess` Esta política permite administrar AWS WAF los recursos de la AWS consola y otros AWS recursos en su nombre en AWS WAF los servicios integrados y dentro de ellos. Detalles en la consola de IAM: AWSWAFConsoleFullAccess.	Permisos ampliados para corregir la configuración de acceso a los AWS App Runner servicios.	06-06-2020
`AWSWAFConsoleReadOnlyAccess` Esta política permite administrar AWS WAF los recursos de la AWS consola y otros AWS recursos en su nombre en AWS WAF los servicios integrados y dentro de ellos. Detalles en la consola de IAM: AWSWAFConsoleReadOnlyAccess.	Permisos ampliados para corregir la configuración de acceso a los AWS App Runner servicios.	06-06-2020
`AWSWAFFullAccess` Esta política le permite administrar AWS WAF los AWS recursos en su nombre en AWS WAF los servicios integrados y dentro de ellos. Detalles en la consola de IAM: AWSWAFFullAccess.	Permisos ampliados para agregar AWS App Runner servicios a los tipos de recursos con AWS WAF los que puede protegerse.	30 de marzo de 2023

Política	Descripción del cambio	Date
`AWSWAFReadOnlyAccess` Esta política le permite administrar AWS WAF los AWS recursos en su nombre en los servicios integrados AWS WAF y dentro de ellos. Detalles en la consola de IAM: AWSWAFReadOnlyAccess.	Permisos ampliados para agregar AWS App Runner servicios a los tipos de recursos con AWS WAF los que puede protegerse.	30 de marzo de 2023
`AWSWAFConsoleFullAccess` Esta política permite AWS WAF administrar los recursos de la AWS consola y otros AWS recursos en su nombre en los servicios integrados AWS WAF y dentro de ellos. Detalles en la consola de IAM: AWSWAFConsoleFullAccess.	Permisos ampliados para agregar AWS App Runner servicios a los tipos de recursos con AWS WAF los que puede protegerse.	30 de marzo de 2023
`AWSWAFConsoleReadOnlyAccess` Esta política permite AWS WAF administrar los recursos de la AWS consola y otros AWS recursos en su nombre en los servicios integrados AWS WAF y dentro de ellos. Detalles en la consola de IAM: AWSWAFConsoleReadOnlyAccess.	Permisos ampliados para agregar AWS App Runner servicios a los tipos de recursos con AWS WAF los que puede protegerse.	30 de marzo de 2023

Política	Descripción del cambio	Date
`AWSWAFFullAccess` Esta política le permite administrar AWS WAF los AWS recursos en su nombre en los servicios integrados AWS WAF y dentro de ellos. Detalles en la consola de IAM: AWSWAFFullAccess.	Permisos ampliados para añadir grupos de usuarios de Amazon Cognito a los tipos de recursos con los que puede protegerse. AWS WAF	25 de agosto de 2022
`AWSWAFReadOnlyAccess` Esta política permite administrar AWS WAF los AWS recursos en su nombre en los servicios integrados AWS WAF y dentro de ellos. Detalles en la consola de IAM: AWSWAFReadOnlyAccess.	Permisos ampliados para añadir grupos de usuarios de Amazon Cognito a los tipos de recursos con los que puede protegerse. AWS WAF	25 de agosto de 2022
`AWSWAFConsoleFullAccess` Esta política permite AWS WAF administrar los recursos de AWS la consola y otros AWS recursos en su nombre en los servicios integrados AWS WAF y dentro de ellos. Detalles en la consola de IAM: AWSWAFConsoleFullAccess.	Permisos ampliados para añadir grupos de usuarios de Amazon Cognito a los tipos de recursos con los que puede protegerse. AWS WAF	25 de agosto de 2022

Política	Descripción del cambio	Date
`AWSWAFConsoleReadOnlyAccess` Esta política permite AWS WAF administrar los recursos de AWS la consola y otros AWS recursos en su nombre en los servicios integrados AWS WAF y dentro de ellos. Detalles en la consola de IAM: AWSWAFConsoleReadOnlyAccess.	Permisos ampliados para añadir grupos de usuarios de Amazon Cognito a los tipos de recursos con los que puede protegerse. AWS WAF	25 de agosto de 2022
`AWSWAFFullAccess` Esta política permite administrar AWS WAF los AWS recursos en su nombre en los servicios integrados AWS WAF y dentro de ellos. Detalles en la consola de IAM: AWSWAFFullAccess.	Se corrigió la configuración de permisos para la entrega de registros para Amazon Simple Storage Service (Amazon S3) y Amazon CloudWatch Logs. Este cambio resuelve los errores de acceso denegado que se produjeron durante la configuración del registro. Para obtener información sobre cómo registrar el tráfico de la ACL web, consulte Registro del tráfico de ACL AWS WAF web.	11/01/2022

Política	Descripción del cambio	Date
`AWSWAFConsoleFullAccess` Esta política permite AWS WAF administrar los recursos de AWS la consola y otros AWS recursos en su nombre en los servicios integrados AWS WAF y dentro de ellos. Detalles en la consola de IAM: AWSWAFConsoleFullAccess.	Se corrigió la configuración de permisos para la entrega de registros para Amazon Simple Storage Service (Amazon S3) y Amazon CloudWatch Logs. Este cambio resuelve los errores de acceso que se produjeron durante la configuración del registro. Para obtener información sobre cómo registrar el tráfico de la ACL web, consulte Registro del tráfico de ACL AWS WAF web.	11/01/2022
`AWSWAFFullAccess` Esta política permite administrar AWS WAF los AWS recursos en su nombre en los servicios integrados AWS WAF y dentro de ellos. Detalles en la consola de IAM: AWSWAFFullAccess.	Se agregaron nuevos permisos para ampliar las opciones de registro. Este cambio da AWS WAF acceso a los destinos de registro adicionales Amazon Simple Storage Service (Amazon S3) y Amazon CloudWatch Logs. Para obtener información sobre cómo registrar el tráfico de la ACL web, consulte Registro del tráfico de ACL AWS WAF web.	15-11-2021

Política	Descripción del cambio	Date
`AWSWAFConsoleFullAccess` Esta política permite AWS WAF administrar los recursos de AWS la consola y otros AWS recursos en su nombre en los servicios integrados AWS WAF y dentro de ellos. Detalles en la consola de IAM: AWSWAFConsoleFullAccess.	Se agregaron nuevos permisos para ampliar las opciones de registro. Este cambio da AWS WAF acceso a los destinos de registro adicionales Amazon Simple Storage Service (Amazon S3) y Amazon CloudWatch Logs. Para obtener información sobre cómo registrar el tráfico de la ACL web, consulte Registro del tráfico de ACL AWS WAF web.	15-11-2021
AWS WAF comenzó a rastrear los cambios	AWS WAF comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	01/03/2021

Solución de problemas AWS WAF de identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con un AWS WAF IAM.

Temas

- No estoy autorizado a realizar ninguna acción en AWS WAF
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS WAF recursos

No estoy autorizado a realizar ninguna acción en AWS WAF

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `wafv2:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 wafv2:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `wafv2:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a AWS WAF.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS WAF. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS WAF recursos

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que

asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si AWS WAF es compatible con estas funciones, consulteCómo AWS WAF funciona con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Uso de roles vinculados a servicios para AWS WAF

AWS WAF usa roles vinculados al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS WAF Los roles vinculados al servicio están predefinidos AWS WAF e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración AWS WAF , ya que no es necesario añadir manualmente los permisos necesarios. AWS WAF define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS WAF puede asumir sus funciones. Los permisos definidos incluyen la política de confianza y la política de permisos. Dicha política de permisos no se puede asociar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a un servicio después de eliminar los recursos relacionados del rol. Esto protege sus AWS WAF recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a un servicio. Seleccione una opción Sí con un enlace para ver la documentación relativa al rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios de AWS WAF

AWS WAF usa la función vinculada al servicio. `AWSServiceRoleForWAFV2Logging`

AWS WAF utiliza esta función vinculada a un servicio para escribir registros en Amazon Data Firehose. Esta función solo se usa si habilita el inicio de sesión. AWS WAF Para obtener más información, consulte Registro del tráfico de ACL AWS WAF web.

El rol vinculado a servicios `AWSServiceRoleForWAFV2Logging` confía en el servicio `wafv2.amazonaws.com` para asumir el rol.

Las políticas de permisos del rol permiten AWS WAF realizar las siguientes acciones en los recursos especificados:

- Acción: `firehose:PutRecord` y `firehose:PutRecordBatch` en Amazon Data Firehose, los recursos de transmisión de datos con un nombre que comience por «aws-waf-logs-». Por ejemplo, `aws-waf-logs-us-east-2-analytics`.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio de AWS WAF

No necesita crear manualmente un rol vinculado a servicios. Cuando habilita el AWS WAF inicio de sesión AWS Management Console, o realiza una `PutLoggingConfiguration` solicitud en la AWS WAF CLI o la AWS WAF API, AWS WAF crea el rol vinculado al servicio para usted.

Debe tener el permiso `iam:CreateServiceLinkedRole` para habilitar el registro.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al habilitar el AWS WAF registro, vuelve a AWS WAF crear el rol vinculado al servicio para usted.

Modificación de un rol vinculado a servicios de AWS WAF

AWS WAF no le permite editar el rol vinculado al `AWSServiceRoleForWAFV2Logging` servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol utilizando IAM. Para obtener más información, consulte Modificación de un rol vinculado a servicios en la Guía del usuario de IAM..

Eliminación de un rol vinculado a un servicio de AWS WAF

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se monitorice ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el AWS WAF servicio utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar AWS WAF los recursos utilizados por el **`AWSServiceRoleForWAFV2Logging`**

1. En la AWS WAF consola, elimine el registro de todas las ACL web. Para obtener más información, consulte Registro del tráfico de ACL AWS WAF web.
2. Mediante la API o la CLI, envíe una solicitud `DeleteLoggingConfiguration` para cada ACL web que tenga habilitado el registro. Para obtener más información, consulte Referencia de la API de AWS WAF.

Cómo eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la CLI de IAM o la API de IAM para eliminar el rol vinculado a servicios `AWSServiceRoleForWAFV2Logging`. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de AWS WAF

AWS WAF admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte Puntos de conexión y cuotas de AWS WAF.

Inicio de sesión y supervisión AWS WAF

El monitoreo es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de AWS WAF sus AWS soluciones. Debe recopilar los datos de supervisión de todas las partes de la AWS solución para poder depurar con mayor facilidad una falla multipunto en caso de que se produzca. AWS proporciona varias herramientas para supervisar sus AWS WAF recursos y responder a posibles eventos:

CloudWatch Alarmas Amazon

Al usar CloudWatch las alarmas, puede observar una única métrica durante un período de tiempo que especifique. Si la métrica supera un umbral determinado, CloudWatch envía una notificación a un tema o AWS Auto Scaling política de Amazon SNS. Para obtener más información, consulte Monitorización con Amazon CloudWatch.

AWS CloudTrail registros

CloudTrail proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en AWS WAF. Con la información recopilada CloudTrail, puede determinar el destinatario de la solicitud AWS WAF, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales. Para obtener más información, consulte Registro de llamadas a la API de AWS CloudTrail con.

AWS WAF registro del tráfico de ACL web

AWS WAF ofrece un registro del tráfico que analizan sus ACL web. Los registros incluyen información como la hora a la que se AWS WAF recibió la solicitud del AWS recurso protegido, información detallada sobre la solicitud y la configuración de la acción de la regla con la que coincidió la solicitud. Para obtener más información, consulte Registro del tráfico de ACL AWS WAF web.

Validación de conformidad para AWS WAF

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

  > **Note**
  >
  > No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos

de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.

- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en AWS WAF

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Seguridad de la infraestructura en AWS WAF

Como servicio gestionado, AWS WAF está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a AWS WAF través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

AWS WAF cuotas

> **Note**
>
> Esta es la última versión de AWS WAF. Para la AWS WAF versión clásica, consulteAWS WAF Clásico.

AWS WAF está sujeto a las siguientes cuotas (anteriormente denominadas límites). Estas cuotas son las mismas para todas las regiones en las que AWS WAF está disponible. Cada región está sujeta a estas cuotas de manera individual. Las cuotas no se acumulan en diferentes regiones.

AWS WAF tiene cuotas predeterminadas para el número máximo de entidades que puede tener por cuenta. Puede solicitar un aumento de dichas cuotas.

Recurso	Cuota predeterminada por cuenta y región
Número máximo de webs ACL	100
Número máximo de grupos de reglas	100
Número máximo de conjuntos de IP	100
Número máximo de solicitudes por segundo por ACL	25 000
Número máximo de encabezados de solicitud personalizados por ACL web o grupo de reglas	100
Número máximo de encabezados de respuesta personalizados por ACL web o grupo de reglas	100
Número máximo de cuerpos de respuesta personalizados por ACL web o grupo de reglas	50
Número máximo de dominios de tokens en una lista de dominios de tokens de la ACL web	10

El número máximo de solicitudes por segundo (RPS) permitido CloudFront está establecido CloudFront y descrito en la Guía para AWS WAF CloudFront desarrolladores.

AWS WAF tiene cuotas fijas en las siguientes configuraciones de entidades por cuenta y región. Estas cuotas no se pueden cambiar.

Recurso	Cuota por cuenta y región
Unidades de capacidad de ACL web (WCU) máxima por ACL web*	5 000
WCU máximo por grupo de reglas	5 000
Número máximo de instrucciones de referencia por grupo de reglas. En un grupo de reglas, una instrucción de referencia puede hacer referencia a un conjunto de direcciones IP o a un conjunto de patrones de regex.	50
Número máximo de instrucciones de referencia por ACL web. En una ACL web, una instrucción de referencia puede hacer referencia a un grupo de reglas, un conjunto de direcciones IP o a un conjunto de patrones de expresiones regulares.	50
Número máximo de direcciones IP en notación CIDR por conjunto de IP	10 000
Número máximo de reglas basadas en tasas por ACL web	10
Número máximo de reglas basadas en tasas	4
Frecuencia de solicitudes mínima que se puede definir para una regla basada en frecuencia	100
Número máximo de direcciones IP únicas a las que se puede limitar las tasas mediante una regla basada en tasas	10 000
Máximo de caracteres para una instrucción de coincidencia de cadena	200
Máximo de caracteres permitidos para cada patrón de expresión regular	200
Número máximo de patrones de expresiones regulares únicos por conjunto de expresiones regulares	10

Recurso	Cuota por cuenta y región
Número máximo de conjuntos de regex	10
Tamaño máximo del cuerpo de una solicitud web que se puede inspeccionar para comprobar si Application Load Balancer y sus protecciones AWS AppSync	8 KB
Tamaño máximo del cuerpo de una solicitud web que se puede inspeccionar CloudFront, así como protecciones de API Gateway, Amazon Cognito, App Runner y Verified Access**	64 KB
Número máximo de transformaciones de texto por instrucción de regla	10
Tamaño máximo del contenido del cuerpo de la respuesta personalizada para una única definición de respuesta personalizada	4 KB
Número máximo de encabezados personalizados para una única definición de respuesta personalizada	10
Número máximo de encabezados personalizados para una única definición de solicitud	10
Tamaño máximo combinado de todo el contenido del cuerpo de la respuesta para un solo grupo de reglas o una única ACL web	50 KB

*El uso de más de 1500 WCU en una ACL web conlleva costos superiores al precio de la ACL web básica. Para obtener más información, consulte AWS WAF unidades de capacidad ACL web (WCU) y Precios de AWS WAF.

**De forma predeterminada, el límite de inspección corporal está establecido en 16 KB para CloudFront los recursos de API Gateway, Amazon Cognito, App Runner y Verified Access, pero puede aumentarlo para cualquiera de estos recursos en su configuración de ACL web, hasta el máximo indicado. Para obtener más información, consulte Gestión de los límites de tamaño de la inspección corporal.

AWS WAF tiene las siguientes cuotas fijas de llamadas por cuenta y región. Estas cuotas se aplican al total de llamadas que se realizan al servicio a través de cualquier medio disponible, como la consola, la CLI, AWS CloudFormation, la API REST y los SDK. Estas cuotas no se pueden cambiar.

Tipo de llamada	Cuota por cuenta y región
Número máximo de llamadas a `AssociateWebACL`	Una solicitud cada 2 segundos
Número máximo de llamadas a `DisassociateWebACL`	Una solicitud cada 2 segundos
Número máximo de llamadas a `GetWebACLForResource`	Una solicitud por segundo
Número máximo de llamadas a `ListResourcesForWebACL`	Una solicitud por segundo
Número máximo de llamadas a cualquier acción `Get` o `List` individual, si no se define ninguna otra cuota.	Cinco solicitudes por segundo
Número máximo de llamadas a cualquier acción `Create`, `Put` o `Update` individual, si no se define ninguna otra cuota.	Una solicitud por segundo

Migración de sus recursos AWS WAF clásicos a AWS WAF

En esta sección se proporcionan instrucciones para migrar las reglas y las ACL web de la AWS WAF versión clásica a. AWS WAF AWS WAF se lanzó en noviembre de 2019. Si ha creado recursos como reglas y ACL web con la versión AWS WAF clásica, tendrá que trabajar con ellos mediante la versión AWS WAF clásica o migrarlos a la última versión.

Antes de iniciar el trabajo de migración, familiarícese con AWS WAF esta lectura. AWS WAF

Temas

- ¿Por qué migrar a AWS WAF?
- Cómo funciona la migración
- Advertencias y limitaciones de la migración

- Migración de una ACL web de la AWS WAF versión clásica a AWS WAF

¿Por qué migrar a AWS WAF?

La última versión de AWS WAF ofrece muchas mejoras con respecto a la versión anterior y, al mismo tiempo, mantiene la mayoría de los conceptos y la terminología a los que está acostumbrado.

En la lista siguiente, se describen los principales cambios de la última versión de AWS WAF. Antes de continuar con la migración, tómese un tiempo para revisar esta lista y familiarizarse con el resto de la AWS WAF guía.

- AWS Reglas administradas para AWS WAF: los grupos de reglas que ahora están disponibles en AWS Managed Rules brindan protección contra las amenazas web más comunes. La mayoría de estos grupos de reglas se incluyen de forma gratuita en AWS WAF. Para obtener más información, consulte AWS Lista de grupos de reglas de Managed Rules y la entrada del blog Anuncie AWS Managed Rules for AWS WAF.
- Nueva AWS WAF API: la nueva API le permite configurar todos sus AWS WAF recursos mediante un único conjunto de API. Para distinguir entre aplicaciones regionales y globales, la nueva API incluye la opción `scope`. Para obtener más información sobre la API, consulte las acciones de WAFV2 de AWS y los tipos de datos de WAFV2 de AWS.

  En las API, los SDK, las CLI y AWS CloudFormation la versión AWS WAF clásica conserva sus esquemas de nomenclatura y AWS WAF se hace referencia a esta última versión con un `V2` o agregado`v2`, según el contexto.
- Cuotas de servicio (límites) simplificadas: AWS WAF ahora permiten más reglas por ACL web y permiten expresar patrones de expresiones regulares más largos. Para obtener más información, consulte AWS WAF cuotas.
- Los límites de las ACL web ahora se basan en las necesidades informáticas; los límites de las ACL web ahora se basan en las unidades de capacidad de las ACL web (WCU). AWS WAF calcula la WCU de una regla en función de la capacidad operativa necesaria para ejecutarla. La WCU de una ACL web es la suma de las WCU de todas las reglas y grupos de reglas de la ACL web.

  Para obtener información general sobre las WCU, consulte Cómo AWS WAF funciona. Para obtener información sobre el uso de las WCU de cada regla, consulte Conceptos básicos de las instrucciones de regla.
- Redacción de reglas basada en documentos: ahora, puede escribir y expresar reglas, grupos de reglas y ACL web en formato JSON. Ya no es necesario utilizar llamadas individuales a las API

para crear condiciones diferentes y asociarlas después a una regla. Esto simplifica enormemente la forma en que escribe y se mantiene el código. Si cuando esté viendo la ACL web desea acceder a las ACL web en formato JSON a través de la consola, elija Download web ACL as JSON (Descargar ACL web como JSON). Cuando cree su propia regla, podrá acceder a su representación JSON con la opción Rule JSON editor (Editor JSON de reglas).

- Anidación de reglas y compatibilidad total con las operaciones lógicas: puede escribir reglas combinadas complejas mediante instrucciones de reglas lógicas y mediante la anidación. Puede crear instrucciones como `[A AND NOT(B OR C)]`. Para obtener más información, consulte instrucciones de reglas lógicas.
- Reglas mejoradas basadas en tasas: en la última versión de AWS WAF, puede personalizar el intervalo de tiempo que evalúa la regla y la forma en que la regla agrega las solicitudes. Puede personalizar la agregación mediante combinaciones de varias características de las solicitudes web. Además, las últimas reglas basadas en tarifas reaccionan más rápidamente a los cambios en el tráfico. Para obtener más información, consulte Instrucción de regla basada en frecuencia.
- Compatibilidad de rangos de CIDR variable para conjuntos de IP: las especificaciones de conjuntos de IP ahora tienen más flexibilidad en los rangos de IP. En el caso de IPv4, AWS WAF es compatible con`/1`. `/32` Para IPv6, AWS WAF es compatible con`/1`. `/128` Para obtener más información sobre los conjuntos de IP, consulte Instrucción de regla de coincidencia de conjuntos de IP.
- Transformaciones de texto encadenables: AWS WAF puede realizar múltiples transformaciones de texto en el contenido de las solicitudes web antes de inspeccionarlo. Para obtener más información, consulte Opciones de transformación de texto.
- Experiencia de consola mejorada: la nueva AWS WAF consola incluye un generador visual de reglas y un diseño de consola más intuitivo para el usuario.
- Opciones ampliadas para AWS WAF las políticas del Firewall Manager: en la administración de las ACL AWS WAF web del Firewall Manager, ahora puede crear un conjunto de grupos de reglas que AWS WAF procesen primero y un conjunto de grupos de reglas que AWS WAF procese en último lugar. Tras aplicar la AWS WAF política, los propietarios de las cuentas locales pueden añadir sus propios grupos de reglas para AWS WAF procesarlos entre estos dos conjuntos. Para obtener más información acerca de las políticas de Firewall Manager de AWS WAF , consulte AWS WAF políticas.
- AWS CloudFormation admite todos los tipos de declaraciones de reglas: AWS WAF AWS CloudFormation admite todos los tipos de declaraciones de reglas compatibles con la AWS WAF consola y la API. Además, puede convertir fácilmente a YAML las reglas que cree en formato JSON.

Cómo funciona la migración

La migración automatizada transfiere la mayor parte de la configuración de ACL web AWS WAF clásica, dejando algunas cosas que debe gestionar manualmente.

A continuación, se indican los pasos generales para migrar una ACL web.

1. La migración automática lee todo lo relacionado con su ACL web actual, sin modificar ni eliminar nada en la AWS WAF versión clásica. Crea una representación de la ACL web y sus recursos relacionados, compatible con AWS WAF. Genera una plantilla de AWS CloudFormation para la nueva ACL web y la almacena en un bucket de Amazon S3.
2. La plantilla se despliega en AWS CloudFormation, para recrear la ACL web y los recursos relacionados en AWS WAF ella.
3. Revise la ACL web y complete manualmente la migración, asegurándose de que la nueva ACL web aproveche al máximo las funcionalidades de la última versión de AWS WAF.
4. Cambie manualmente los recursos protegidos a la nueva ACL web.

Advertencias y limitaciones de la migración

La migración no traspasa toda la configuración exactamente igual que está en AWS WAF Classic. Algunas cosas, como las reglas administradas, no tienen una correspondencia exacta entre las dos versiones. Otras opciones, como las asociaciones de la ACL web con los recursos protegidos de AWS , inicialmente están deshabilitadas en la nueva versión para que pueda agregarlas cuando todo esté listo.

En la lista siguiente, se describen las advertencias de la migración y los pasos que tal vez desee realizar en respuesta. Utilice esta información general para planificar la migración. Más adelante, encontrará pasos detallados sobre la migración, que le servirán de ayuda para efectuar las operaciones de mitigación recomendadas.

- Cuenta única: solo puede migrar los recursos AWS WAF clásicos de cualquier cuenta a AWS WAF los recursos de la misma cuenta.
- Reglas gestionadas: la migración no incorpora ninguna regla gestionada por parte de AWS Marketplace los vendedores. Algunos AWS Marketplace vendedores tienen reglas de gestión equivalentes a las AWS WAF que puedes volver a suscribirte. Antes de hacerlo, consulta las reglas AWS gestionadas que se incluyen en la versión más reciente de AWS WAF. La mayoría

de ellas son gratuitas para AWS WAF los usuarios. Para obtener información sobre las reglas administradas, consulte Grupos de reglas administrados.

- Asociaciones de la ACL web: la migración no implica ninguna asociación entre la ACL web y los recursos protegidos. Esto es así por diseño, para evitar que la carga de trabajo de producción se vea afectada. Cuando compruebe que todo se ha migrado correctamente, asocie la nueva ACL web con los recursos.
- Registro: el registro de la ACL web migrada está deshabilitado de forma predeterminada. Este comportamiento es así por diseño. Habilite el registro cuando esté listo para cambiar de la AWS WAF versión clásica a AWS WAF.
- AWS Firewall Manager grupos de reglas: la migración no gestiona los grupos de reglas que administra Firewall Manager. Puede migrar una ACL web administrada por Firewall Manager, pero el grupo de reglas no se migrará. En lugar de utilizar la herramienta de migración con estas ACL web, vuelva a crear la política de la nueva versión de AWS WAF en Firewall Manager.

  > **Note**
  >
  > Los grupos de reglas que administraba Firewall Manager para la AWS WAF versión clásica eran grupos de reglas de Firewall Manager. Con la nueva versión de AWS WAF, los grupos de reglas son grupos de AWS WAF reglas. Desde el punto de vista funcional, esto no supone ningún cambio.

- AWS WAF Automatizaciones de seguridad: no intente migrar ninguna automatización AWS WAF de seguridad. La migración no convierte las funciones Lambda, que podrían estar utilizándose en las automatizaciones. Cuando haya disponible una nueva solución de automatización de AWS WAF seguridad que sea compatible con la última AWS WAF, vuelva a implementarla.

Migración de una ACL web de la AWS WAF versión clásica a AWS WAF

Para migrar una ACL web y cambiar a ella, realice primero la migración automatizada y efectúe después los pasos manuales.

Temas

- Migración de una ACL web: migración automatizada
- Migración de una ACL web: seguimiento manual
- Migración de una ACL web: consideraciones adicionales
- Migración de una ACL web: cambio

Migración de una ACL web: migración automatizada

Para migrar automáticamente una configuración de ACL web de AWS WAF Classic a AWS WAF

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.
2. Elija Cambiar a la AWS WAF versión clásica y revise los ajustes de configuración de la ACL web. Anote los valores atendiendo a las advertencias y limitaciones que se indican en la sección anterior, Advertencias y limitaciones de la migración.
3. En el cuadro de diálogo informativo de la parte superior, busque la frase que comienza con Migre la ACL web y seleccione el enlace al asistente de migración. Al hacerlo, se abrirá el asistente de migración.

   Si no ve el cuadro de diálogo informativo, es posible que lo haya cerrado desde que lanzó la consola AWS WAF clásica. En la barra de navegación, selecciona Cambiar a nueva y, a AWS WAF continuación, selecciona Cambiar a AWS WAF clásica y volverá a aparecer el cuadro de diálogo informativo.
4. Seleccione la ACL web que desee migrar.
5. En Configuración de la migración, indique un bucket de Amazon S3 que desee usar con la plantilla. Necesita un bucket de Amazon S3 que esté configurado correctamente para la API de migración para almacenar la AWS CloudFormation plantilla que genera.

   - Si el bucket está cifrado, debe utilizar claves de Amazon S3 (SSE-S3). La migración no admite el cifrado con claves AWS Key Management Service (SSE-KMS).
   - El nombre del bucket debe comenzar por `aws-waf-migration-`. Por ejemplo, `aws-waf-migration-my-web-acl`.
   - El bucket debe estar en la región en la que se va a implementar la plantilla. Por ejemplo, en una ACL web de `us-west-2`, deberá usar un bucket de Amazon S3 que esté en `us-west-2` y debe implementar la pila de la plantilla en `us-west-2`.
6. En la política del bucket de S3, es recomendable elegir Auto apply the bucket policy required for migration (Aplicar automáticamente la política de bucket necesaria para la migración). Si lo desea, también puede administrar el bucket por su cuenta. Para ello, debe aplicar manualmente la siguiente política de bucket:

   - Para CloudFront aplicaciones globales de Amazon (`waf`):

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "apiv2migration.waf.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/
*"
        }
    ]
}
```

- Para aplicaciones regionales de Amazon API Gateway o el equilibrador de carga de aplicación (`waf-regional`):

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "apiv2migration.waf-regional.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/
*"
        }
    ]
}
```

7. En Choose how to handle rules that cannot be migrated (Elija cómo desea administrar las reglas que no se pueden migrar), elija si desea excluir las reglas que no se pueden migrar o detener la migración. Para obtener más información sobre las reglas que no se pueden migrar, consulte Advertencias y limitaciones de la migración.
8. Elija Siguiente.
9. En Crear AWS CloudFormation plantilla, verifica la configuración y, a continuación, selecciona Empezar a crear AWS CloudFormation plantilla para iniciar el proceso de migración. Esto puede tardar unos minutos, en función de la complejidad de la ACL web.

10. En Crear y ejecutar una AWS CloudFormation pila para completar la migración, puede optar por ir a la AWS CloudFormation consola para crear una pila a partir de la plantilla y crear la nueva ACL web y sus recursos. Para ello, elija Crear AWS CloudFormation pila.

Cuando se complete el proceso de migración automática, estará todo listo para continuar con los pasos manuales. Consulte Migración de una ACL web: seguimiento manual.

Migración de una ACL web: seguimiento manual

Una vez finalizada la migración automatizada, revise la ACL web recién creada y complete los componentes que no se pudieron migrar. El siguiente procedimiento cubre los aspectos de la administración de ACL web que la migración no abarca. Para ver la lista, consulte Advertencias y limitaciones de la migración.

Para finalizar la migración básica (pasos manuales)

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.
2. La consola debería usar automáticamente la última versión de AWS WAF. Para comprobarlo, en el panel de navegación, compruebe que puede ver la opción Cambiar a la AWS WAF versión clásica. Si aparece Cambiar a una versión nueva AWS WAF, selecciónela para cambiar a la versión más reciente.
3. En el panel de navegación, seleccione Web ACLs (ACL web).
4. En la página Web ACLs (ACL web), busque la nueva ACL web en la lista de la región donde la creó. Elija el nombre de la ACL web para abrir la configuración.
5. Compare todos los ajustes de la nueva ACL web con su ACL web AWS WAF clásica anterior. De forma predeterminada, el registro y las asociaciones de recursos protegidos estarán deshabilitados. Se habilitarán cuando esté todo listo para cambiar a la nueva versión.
6. Si su ACL web AWS WAF clásica tenía una regla basada en la velocidad con una condición, la condición no se introdujo en la migración. Puede agregar condiciones a la regla de la nueva ACL web.

    a. En la página de configuración de la ACL web, elija la pestaña Rules (Reglas).

    b. Busque en la lista la regla basada en frecuencia, selecciónela y elija Edit (Editar).

    c. En Criteria to count request towards rate limit (Criterios para incluir la solicitud en el cálculo de los límites de frecuencia), seleccione Only consider requests that match the

criteria in a rule statement (Tener en cuenta solo las solicitudes que coincidan con los criterios de la instrucción de una regla) e incluya los criterios adicionales que desee. Puede agregar criterios utilizando cualquier instrucción de regla que se pueda anidar, como las instrucciones lógicas. Para obtener información sobre sus opciones, consulte Instrucción de regla basada en frecuencia.

7. Si su ACL web AWS WAF clásica tenía un grupo de reglas administrado, la inclusión del grupo de reglas no se incorporó en la migración. Puede agregar grupos de reglas administradas a la nueva ACL web. Consulte la información sobre los grupos de reglas administrados, incluida la lista de reglas AWS administradas que están disponibles con la nueva versión de AWS WAF, enGrupos de reglas administrados. Para agregar un grupo de reglas administradas, haga lo siguiente:

   a. En la página de configuración de la ACL web, elija la pestaña Rules (Reglas).

   b. Elija Add Rules (Agregar reglas) y Add managed rule groups (Agregar grupos de reglas administradas).

   c. Expanda el listado del proveedor que prefiera y seleccione los grupos de reglas que desee agregar. En el AWS Marketplace caso de los vendedores, es posible que tengas que suscribirte a los grupos de reglas. Para obtener más información sobre el uso de grupos de reglas administradas en la ACL web, consulte Grupos de reglas administrados y Evaluación de reglas y grupos de reglas de ACL web.

Una vez finalizado el proceso básico de migración, le recomendamos que revise sus necesidades y considere otras opciones para asegurarse de que la nueva configuración es lo más eficiente posible y que está utilizando las últimas opciones de seguridad disponibles. Consulte Migración de una ACL web: consideraciones adicionales.

Migración de una ACL web: consideraciones adicionales

Revise su nueva ACL web y considere las opciones disponibles en la nueva AWS WAF para asegurarse de que la configuración sea lo más eficiente posible y de que utilice las últimas opciones de seguridad disponibles.

Reglas AWS administradas adicionales

Considere la posibilidad de implementar reglas AWS administradas adicionales en su ACL web para aumentar la seguridad de su aplicación. Se incluyen sin AWS WAF costo adicional. AWS Las reglas administradas incluyen los siguientes tipos de grupos de reglas:

- Los grupos de reglas base proporcionan protección general contra una serie de amenazas comunes, como impedir que se realicen entradas incorrectas conocidas en la aplicación o impedir el acceso a la página de administración.
- Los grupos de reglas específicos para los casos de uso proporcionan mayor protección para diversos y numerosos escenarios y entornos.
- Las listas de reputación de IP proporcionan información sobre las amenazas en función de la IP de origen del cliente.

Para obtener más información, consulte AWS Reglas administradas para AWS WAF.

Optimización y limpieza de reglas

Vuelva a revisar las reglas antiguas y considere la posibilidad de optimizarlas reescribiéndolas o eliminando las que estén obsoletas. Por ejemplo, si en el pasado implementó una AWS CloudFormation plantilla del documento técnico sobre las 10 principales vulnerabilidades de aplicaciones web de OWASP, Prepare for the OWASP Top 10 Vulnerability Vulnerability Using AWS WAF y Our New White Paper, debería considerar la posibilidad de sustituirla por reglas administradas. AWS Si bien el concepto incluido en el documento sigue siendo aplicable y puede ayudarle a redactar sus propias reglas, las reglas creadas por la plantilla han sido reemplazadas en gran medida por las reglas administradas. AWS

CloudWatch Métricas y alarmas de Amazon

Revisa tus CloudWatch estadísticas de Amazon y configura las alarmas según sea necesario. La migración no transfiere las CloudWatch alarmas y es posible que los nombres de tus métricas no sean los que deseas.

Revisión con el equipo de aplicaciones

Trabaje con su equipo de aplicaciones y compruebe su enfoque en materia de seguridad. Averigüe qué campos analiza con frecuencia la aplicación y agregue reglas para limpiar la entrada como corresponda. Compruebe si hay casos perimetrales y agregue reglas para detectar estos casos si la lógica de negocio de la aplicación no puede procesarlos.

Planificación del cambio

Planifique el momento en que se va a realizar el cambio con el equipo de aplicaciones. El cambio de la antigua asociación de ACL web a la nueva puede tardar un poco en propagarse a todas las áreas en las que se almacenan los recursos. El tiempo de propagación puede oscilar entre unos segundos

y varios minutos. Durante este tiempo, la antigua ACL web procesará algunas solicitudes y la nueva ACL web procesará otras. Sus recursos estarán protegidos durante todo el cambio, pero es posible que observe incoherencias en la gestión de las solicitudes mientras el cambio esté en marcha.

Cuando todo esté listo para realizar el cambio, siga el procedimiento que se indica en Migración de una ACL web: cambio.

Migración de una ACL web: cambio

Tras comprobar la nueva configuración de ACL web, puede comenzar a usarla en lugar de la ACL web de AWS WAF Classic.

Para empezar a usar su nueva ACL AWS WAF web

1. Asocie la ACL AWS WAF web a los recursos que desee proteger, siguiendo las instrucciones que se indican enAsociar o desasociar una ACL web a un recurso AWS. De este modo, se interrumpirá automáticamente la asociación de los recursos con la antigua ACL web.

   El cambio puede tardar en propagarse entre unos segundos y varios minutos. Durante este tiempo, la antigua ACL web podrá procesar algunas solicitudes y la nueva ACL web podrá procesar otras. Sus recursos estarán protegidos durante todo el cambio, pero es posible que observe incoherencias en la gestión de las solicitudes hasta que esté completo.
2. Configure el registro de la nueva ACL web siguiendo las instrucciones de Registro del tráfico de ACL AWS WAF web.
3. (Opcional) Si su ACL web AWS WAF clásica ya no está asociada a ningún recurso, considere eliminarla por completo de la AWS WAF versión clásica. Para obtener más información, consulte Eliminación de una ACL web.

AWS WAF Clásico

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la versión más reciente. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

AWS WAF Classic es un firewall de aplicaciones web que le permite supervisar las solicitudes HTTP y HTTPS que se reenvían a una API de Amazon API Gateway, Amazon CloudFront o un Application Load Balancer. AWS WAF Classic también te permite controlar el acceso a tu contenido. Según las condiciones que especifique, como las direcciones IP de las que se originan las solicitudes o los valores de las cadenas de consulta, API Gateway CloudFront o un Application Load Balancer responden a las solicitudes con el contenido solicitado o con un código de estado HTTP 403 (prohibido). También puedes configurarlo CloudFront para que muestre una página de error personalizada cuando se bloquee una solicitud.

Temas

Configuración de AWS WAF Classic

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

En este tema se describen los pasos preliminares, como la creación de una cuenta de usuario, para preparar el uso de la AWS WAF versión clásica. Esto no tiene coste. Solo se le cobrará por AWS los servicios que utilice.

> **Note**
>
> Si eres un usuario nuevo AWS WAF, no sigas estos pasos de configuración para la AWS WAF versión clásica. En su lugar, sigue los pasos de la versión más reciente de AWS WAF, enConfiguración de su cuenta para usar los servicios.

Tras completar estos pasos, consulte Cómo empezar con AWS WAF Classic para continuar con la AWS WAF versión clásica.

> **Note**
>
> AWS Shield Standard se incluye en la AWS WAF versión clásica y no requiere configuración adicional. Para obtener más información, consulte Cómo funcionan AWS Shield and Shield Advanced.

Antes de usar la AWS WAF versión clásica o AWS Shield Advanced por primera vez, complete los pasos de esta sección.

Temas

- Inscríbase en una Cuenta de AWS
- Creación de un usuario con acceso administrativo

- Descargar herramientas

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Signing in as the root user en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Descargar herramientas

AWS Management Console Incluye una consola para AWS WAF Classic, pero si desea acceder a AWS WAF Classic mediante programación, consulte lo siguiente:

- Si quieres llamar a la API AWS WAF clásica sin tener que gestionar detalles de bajo nivel, como el ensamblaje de solicitudes HTTP sin procesar, puedes usar un SDK. AWS Los AWS SDK proporcionan funciones y tipos de datos que encapsulan la funcionalidad de la AWS WAF versión clásica y de otros servicios. AWS Para descargar un AWS SDK, consulta la página correspondiente, que también incluye los requisitos previos y las instrucciones de instalación:
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  Para obtener una lista completa de AWS los SDK, consulte Herramientas para Amazon Web Services.
- Si utilizas un lenguaje de programación para el que AWS no se proporciona un SDK, la referencia de la AWS WAF API documenta las operaciones que admite AWS WAF Classic.
- El AWS Command Line Interface (AWS CLI) es compatible con AWS WAF Classic. AWS CLI Permite controlar varios AWS servicios desde la línea de comandos y automatizarlos mediante scripts. Para obtener más información, consulte AWS Command Line Interface.
- AWS Tools for Windows PowerShell es compatible con AWS WAF Classic. Para obtener más información, consulte Referencia de cmdlet de AWS Tools for PowerShell.

Cómo funciona AWS WAF Classic

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los

ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Utiliza AWS WAF Classic para controlar la forma en que API Gateway, Amazon CloudFront o un Application Load Balancer responden a las solicitudes web. Comience creando condiciones, reglas y listas de control de acceso a la web (ACL a la web). Puede definir sus condiciones, agruparlas en reglas y combinar las reglas en una ACL web.

> **Note**
>
> También puede usar AWS WAF Classic para proteger las aplicaciones alojadas en contenedores de Amazon Elastic Container Service (Amazon ECS). Amazon ECS es un servicio de administración de contenedores muy escalable y rápido que facilita la tarea de ejecutar, detener y administrar contenedores de Docker en un clúster. Para usar esta opción, debe configurar Amazon ECS para que utilice un Application Load Balancer con la AWS WAF versión clásica para enrutar y proteger el tráfico HTTP/HTTPS (capa 7) entre las tareas de su servicio. Para obtener más información, consulte el tema Equilibrio de carga de servicio en la Guía para desarrolladores de Amazon Elastic Container Service.

Condiciones

Las condiciones definen las características básicas que desea que AWS WAF Classic vea en las solicitudes web:

- Scripts que probablemente sean maliciosos. Los atacantes incrustan scripts que pueden aprovechar vulnerabilidades en aplicaciones web. Esto es lo que se conoce como scripts entre sitios.
- Direcciones IP o rangos de direcciones de las que procedan las solicitudes.
- País o ubicación geográfica de donde provienen las solicitudes.
- Longitud de determinadas partes de la solicitud, como la cadena de consulta.
- Código SQL que puede ser malicioso. Los atacantes tratan de extraer los datos de su base de datos incrustando código SQL malicioso en una solicitud web. Esto es lo que se conoce como inyección de código SQL.

- Cadenas que aparecen en la solicitud, por ejemplo, valores que aparecen en el encabezado de `User-Agent` o cadenas de texto que aparecen en la cadena de consulta. También puede utilizar expresiones regulares (regex) para especificar estas cadenas.

Algunas condiciones adoptan valores diversos. Por ejemplo, puede especificar hasta 10,000 direcciones IP o rangos de direcciones de IP en una condición IP.

Reglas

Las condiciones se combinan en reglas para segmentar con precisión las solicitudes que se desean permitir, bloquear o contar. AWS WAF La versión clásica ofrece dos tipos de reglas:

Regla normal

Las reglas normales solo usan condiciones para dirigirse a solicitudes específicas. Por ejemplo, de acuerdo con las últimas solicitudes que haya visto de un atacante, puede crear una regla que incluya las siguientes condiciones:

- Las solicitudes provienen de 192.0.2.44.
- Contienen el valor `BadBot` en el encabezado `User-Agent`.
- Parece que incluyan código tipo SQL en la cadena de consulta.

Cuando una regla incluya varias condiciones, como en este ejemplo, AWS WAF Classic buscará las solicitudes que coincidan con todas las condiciones; es decir, unirá las condiciones mediante `AND`.

Añada al menos una condición para una regla normal. Una regla normal sin condiciones no puede coincidir con ninguna solicitud, por lo que la acción de la regla (permitir, contar o bloquear) nunca se activa.

Regla basada en frecuencia

Las reglas basadas en frecuencia son como las reglas normales con un límite de frecuencia añadido. Una regla basada en frecuencia cuenta las solicitudes que llegan de direcciones IP que cumplen las condiciones de la regla. Si las solicitudes de una dirección IP superan el límite de frecuencia en un periodo de cinco minutos, la regla puede activar una acción. La acción puede tardar uno o dos minutos en activarse.

Sin embargo, las condiciones son opcionales para las reglas basadas en frecuencia. Si no añade ninguna condición a una regla basada en frecuencia, el límite de frecuencia se aplica a todas las direcciones IP. Si combina condiciones con el límite de frecuencia, el límite de frecuencia se aplica a las direcciones IP que coinciden con las condiciones.

Por ejemplo, de acuerdo con las últimas solicitudes que haya visto de un atacante, puede crear una regla basada en frecuencia que incluya las siguientes condiciones:

- Las solicitudes provienen de 192.0.2.44.
- Contienen el valor `BadBot` en el encabezado `User-Agent`.

En esta regla basada en frecuencia defina también un límite de frecuencia. En este ejemplo, supongamos que crea un límite de frecuencia de 1 000. Las solicitudes que cumplan las dos condiciones anteriores y superen las 1 000 solicitudes durante cinco minutos activan la acción de la regla (bloquear o contar), que está definida en la ACL web.

Las solicitudes que no cumplen ambas condiciones no se tienen en cuenta para el límite de frecuencia y no se ven afectadas por esta regla.

Otro ejemplo: suponga que desea limitar las solicitudes de una determinada página de su sitio web. Para ello, podría añadir la siguiente condición de coincidencia de cadena para crear una regla basada en frecuencia:

- El valor de Part of the request to filter on es `URI`.
- El valor de Match Type es `Starts with`.
- El valor de Value to match es `login`.

Además, especifica un `RateLimit` de 1 000.

Al añadir esta regla basada en frecuencia a una ACL web, podría limitar las solicitudes de la página de inicio de sesión sin que se vea afectado el resto del sitio.

ACL de web

Después de combinar sus condiciones en reglas, puede combinar las reglas en una ACL de web. Ahí es donde define una acción para cada regla, permitir, bloquear o contar, y una acción predeterminada:

Una acción para cada regla

Cuando una solicitud web cumple todas las condiciones de una regla, AWS WAF Classic puede bloquear la solicitud o permitir que se reenvíe a la API de API Gateway, a la CloudFront distribución o a un Application Load Balancer. Usted especifica la acción que quiere que AWS WAF Classic lleve a cabo para cada regla.

AWS WAF Classic compara una solicitud con las reglas de una ACL web en el orden en que se enumeraron las reglas. AWS WAF A continuación, Classic realiza la acción asociada a la

primera regla con la que coincide la solicitud. Por ejemplo, si una solicitud web coincide con una regla que permite las solicitudes y otra que bloquea las solicitudes, AWS WAF Classic permitirá o bloqueará la solicitud en función de la regla que aparezca primero.

Si quieres probar una nueva regla antes de empezar a usarla, también puedes configurar AWS WAF Classic para que cuente las solicitudes que cumplen todas las condiciones de la regla. Al igual que ocurre con las reglas que permiten o bloquean solicitudes, una regla que cuenta solicitudes depende de su posición en la lista de reglas de la ACL de web. Por ejemplo, si una solicitud web coincide con una regla que permite solicitudes y otra que cuenta solicitudes; y si la regla que permite las solicitudes está antes, la solicitud no se cuenta.

Una acción predeterminada

La acción predeterminada determina si AWS WAF Classic permite o bloquea una solicitud que no cumpla todas las condiciones de ninguna de las reglas de la ACL web. Por ejemplo, suponga que crea una ACL de web y solo añade la regla que definió antes:

- Las solicitudes provienen de 192.0.2.44.
- Contienen el valor `BadBot` en el encabezado `User-Agent`.
- Parece que incluyan código SQL malicioso en la cadena de consulta.

Si una solicitud no cumple las tres condiciones de la regla y si la acción predeterminada es`ALLOW`, AWS WAF Classic reenvía la solicitud a API Gateway CloudFront o a un Application Load Balancer, y el servicio responde con el objeto solicitado.

Si agregas dos o más reglas a una ACL web, AWS WAF Classic solo realiza la acción predeterminada si la solicitud no cumple todas las condiciones de ninguna de las reglas. Por ejemplo, suponga que agrega una segunda regla que contiene una condición:

- Solicitudes que contienen el valor `BIGBadBot` en el encabezado `User-Agent`.

AWS WAF La versión clásica solo realiza la acción predeterminada cuando una solicitud no cumple las tres condiciones de la primera regla y no cumple una de las condiciones de la segunda regla.

En algunas ocasiones, AWS WAF puede producirse un error interno que retrase la respuesta a Amazon API Gateway, Amazon CloudFront o un Application Load Balancer sobre si se debe permitir o bloquear una solicitud. En esas ocasiones, normalmente CloudFront permitirá la solicitud o servirá el contenido. Una gateway de API y un Balanceador de carga de aplicaciones normalmente denegará la solicitud y no servirá el contenido.

AWS WAF Precios clásicos

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debes usar esta versión si creaste AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los has migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Con AWS WAF Classic, solo paga por las ACL y las reglas web que cree, y por el número de solicitudes HTTP que AWS WAF Classic inspeccione. Para obtener más información, consulte Precios de AWS WAF Classic.

Cómo empezar con AWS WAF Classic

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

En este tutorial se muestra cómo utilizar la AWS WAF versión clásica para realizar las siguientes tareas:

- Configure AWS WAF Classic.
- Cree una lista de control de acceso web (ACL web) mediante la consola AWS WAF clásica y especifique las condiciones que desee utilizar para filtrar las solicitudes web. Por ejemplo, puede especificar las direcciones IP de donde provienen las solicitudes y valores incluidos en la solicitud que solo utilicen los atacantes.
- Añadir las condiciones a una regla. Las reglas le permiten centrarse en las solicitudes web que desea bloquear o permitir. Una solicitud web debe cumplir todas las condiciones de una regla

para que AWS WAF Classic bloquee o permita las solicitudes en función de las condiciones que especifique.

- Añadir las reglas a ACL web. Aquí es donde debe especificar si desea bloquear solicitudes web o permitirlas en función de las condiciones que haya añadido a cada regla.
- Especificar una acción predeterminada, ya sea bloquear o permitir. Esta es la acción que realiza AWS WAF Classic cuando una solicitud web no coincide con ninguna de tus reglas.
- Elige la CloudFront distribución de Amazon para la que quieres que AWS WAF Classic inspeccione las solicitudes web. En este tutorial solo se describen los pasos CloudFront, pero el proceso para las API de Application Load Balancer y Amazon API Gateway es básicamente el mismo. AWS WAF Classic for CloudFront está disponible para todos Regiones de AWS. AWS WAF La versión clásica para su uso con API Gateway o un Application Load Balancer está disponible en las regiones que figuran en los puntos de conexión del AWS servicio.

> **Note**
>
> AWS normalmente te factura menos de 0,25 USD al día por los recursos que crees durante este tutorial. Cuando haya completado el tutorial, le recomendamos que elimine los recursos para evitar incurrir en gastos innecesarios.

Temas

Paso 1: Configura Classic AWS WAF

Si aún no ha seguido los pasos de configuración generales de Configuración de AWS WAF Classic, hágalo ahora.

Paso 2: Crear una ACL web

La consola AWS WAF Classic le guía a través del proceso de configuración de AWS WAF Classic para bloquear o permitir las solicitudes web en función de las condiciones que especifique, como las direcciones IP de las que se originan las solicitudes o los valores de las solicitudes. En este paso, va a crear una ACL web.

Para crear una ACL web

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. Si es la primera vez que usa la AWS WAF versión clásica, elija Ir a la AWS WAF versión clásica y, a continuación, elija Configurar ACL web.

   Si ya ha utilizado la AWS WAF versión clásica, seleccione ACL web en el panel de navegación y, a continuación, elija Crear ACL web.
3. En la página Name web ACL (Nombrar ACL web), escriba un nombre para Web ACL name (Nombre de ACL web).

   > **Note**
   >
   > No se puede cambiar el nombre después de crear la ACL web.

4. Para el nombre de la CloudWatch métrica, introduzca un nombre. El nombre solo puede contener caracteres alfanuméricos (A-Z, a-z y 0-9). No puede contener espacios en blanco.

   > **Note**
   >
   > No se puede cambiar el nombre después de crear la ACL web.

5. En Región, seleccione una región. Si va a asociar esta ACL web a una CloudFront distribución, elija Global (CloudFront).

6. En AWS resource to associate, seleccione el recurso que desea asociar a la ACL web y, a continuación, elija Next.

Paso 3: Crear una condición de coincidencia de IP

Una condición de coincidencia de IP especifica las direcciones IP o los rangos de direcciones IP de donde provienen las solicitudes. En este paso, va a crear una condición de coincidencia de IP. En una paso posterior, indicará si desea permitir o bloquear las solicitudes que provengan de las direcciones IP especificadas.

> **Note**
>
> Para obtener más información acerca de las condiciones de coincidencia de IP, consulte Trabajar con condiciones de coincidencia de IP.

Para crear una condición de coincidencia de IP

1. En la página Create conditions, para IP match conditions, elija Create condition.
2. En el cuadro de diálogo Create IP match condition (Crear condición de coincidencia de IP), escriba un nombre en Name (Nombre). El nombre solo puede contener caracteres alfanuméricos (A-Z, a-z, 0-9) o los siguientes caracteres especiales: _-!"#`+*},./.
3. En Address (Dirección), introduzca 192.0.2.0/24. Este rango de direcciones IP, especificado en notación CIDR, incluye las direcciones IP comprendidas entre 192.0.2.0 y 192.0.2.255. (El rango de direcciones IP 192.0.2.0/24 se reserva a los ejemplos, por lo que no se originarán solicitudes web desde esas direcciones IP).

   AWS WAF Classic admite rangos de direcciones IPv4: /8 y cualquier rango entre /16 y /32. AWS WAF Classic admite los rangos de direcciones IPv6: /24, /32, /48, /56, /64 y /128. (Para especificar una dirección IP única, como 192.0.2.44, escriba 192.0.2.44/32). Los demás rangos no se admiten.

   Para obtener más información acerca de la notación CIDR, consulte el artículo de Wikipedia Classless Inter-Domain Routing.
4. Seleccione Crear.

Paso 4: Crear una condición de coincidencia geográfica

Una condición de coincidencia geográfica especifica el país o los países de los que proceden las solicitudes. En este paso, va a crear una condición de coincidencia geográfica. En un paso posterior, indicará si desea permitir o bloquear las solicitudes que provengan de los países especificados.

> **Note**
>
> Para obtener más información acerca de las condiciones de coincidencia geográfica, consulte Trabajar con condiciones de coincidencia geográfica.

Para crear una condición de coincidencia geográfica

1. En la página Create conditions, en Geo match conditions, elija Create condition.
2. En el cuadro de diálogo Create geo match condition (Crear condición de coincidencia geográfica), escriba un nombre en Name (Nombre). El nombre solo puede contener caracteres alfanuméricos (A-Z, a-z, 0-9) o los siguientes caracteres especiales: _-!"#`+*},./.
3. Elija un valor en Location type (Tipo de ubicación) y un país. Actualmente, el valor Location type (Tipo de ubicación) solo puede ser Country (País).
4. Elija Add location (Agregar ubicación).
5. Seleccione Crear.

Paso 5: Crear una condición de coincidencia de cadena

Una condición de coincidencia de cadenas identifica las cadenas que desea que AWS WAF Classic busque en una solicitud, como un valor especificado en un encabezado o en una cadena de consulta. Normalmente, una cadena se compone de caracteres ASCII imprimibles, pero puede especificar cualquier carácter comprendido entre los valores hexadecimales 0x00 y 0xFF (valores decimales 0 a 255). En este paso, va a crear una condición de coincidencia de cadena. En un paso posterior, especificará si desea permitir o bloquear las solicitudes que contengan las cadenas especificadas.

> **Note**
>
> Para obtener más información acerca de las condiciones de coincidencia de cadena, consulte Trabajar con condiciones de coincidencia de cadena.

Para crear una condición de coincidencia de cadena

1. En la página Create conditions (Crear condiciones), para String y regex match conditions (Condiciones de coincidencia de cadenas y expresiones regulares), elija Create condition (Crear condición).
2. En el cuadro de diálogo Create string match condition (Crear condición de coincidencia de cadena), escriba los valores siguientes:

   Nombre

   Escriba un nombre. El nombre solo puede contener caracteres alfanuméricos (A-Z, a-z, 0-9) o los siguientes caracteres especiales: _-!"#`+*},./.

   Tipo

   Elija Coincidencia de cadena.

   Parte de la solicitud para filtrar en

   Elija la parte de la solicitud web que desee que AWS WAF Classic inspeccione en busca de una cadena específica.

   En este ejemplo, seleccione Header.

   > **Note**
   >
   > Si eliges Body como valor de la parte de la solicitud que deseas filtrar, AWS WAF Classic inspecciona solo los primeros 8192 bytes (8 KB), ya que solo CloudFront reenvía los primeros 8192 bytes para su inspección. Para permitir o bloquear solicitudes cuyo cuerpo tenga más de 8192 bytes, puede crear una condición de restricción de tamaño. (AWS WAF Classic obtiene la longitud del cuerpo de los encabezados de las solicitudes). Para obtener más información, consulte Trabajar con condiciones de restricción de tamaño.

Encabezado (obligatorio si "Parte de la solicitud para filtrar en" es "Encabezado")

Como has elegido el encabezado para filtrar una parte de la solicitud, debes especificar qué encabezado quieres que inspeccione AWS WAF Classic. Introduzca User-Agent (Agente de usuario). (Este valor no distingue entre mayúsculas y minúsculas).

Tipo de coincidencia

Elija en qué punto del encabezado User-Agent debe aparecer la cadena especificada; por ejemplo, al principio, al final o en algún punto de la cadena.

Para este ejemplo, elija Coincidencias exactas, lo que indica que AWS WAF Classic inspecciona las solicitudes web en busca de un valor de encabezado idéntico al valor que usted especifique.

Transformación

Para evitar la AWS WAF versión clásica, los atacantes utilizan un formato inusual en las solicitudes web, por ejemplo, añadiendo espacios en blanco o codificando en URL una parte o la totalidad de las solicitudes. Las transformaciones convierten la solicitud web en un formato más próximo al estándar, ya que eliminan los espacios en blanco, descodifican con URL la solicitud o realizan otras operaciones que eliminan gran parte del formato fuera de lo corriente que los atacantes suelen utilizar.

Solo puede especificar un único tipo de transformación de texto.

En este ejemplo, seleccione None.

El valor se codifica con base64

Si el valor que introduce en Value to match (Valor que debe coincidir) ya tiene una codificación con base64, seleccione esta casilla de verificación.

En este ejemplo, no seleccione la casilla de verificación.

Valor que debe coincidir

Especifica el valor que deseas que AWS WAF Classic busque en la parte de las solicitudes web que indicaste en Parte de la solicitud por la que se va a filtrar.

Para este ejemplo, introduzca BadBot. AWS WAF Classic inspeccionará el `User-Agent` encabezado de las solicitudes web para determinar el valor BadBot.

La longitud máxima de Value to match es 50 caracteres. Si desea especificar un valor con codificación base64, puede proporcionar hasta 50 caracteres antes de la codificación.

3. Si quieres que AWS WAF Classic inspeccione las solicitudes web en busca de varios valores, como un `User-Agent` encabezado que contenga `BadBot` y una cadena de consulta que contenga varios valores`BadParameter`, tienes dos opciones:

   - Si desea permitir o bloquear solicitudes web solo cuando estas contengan ambos valores (`AND`), debe crear una condición de coincidencia de cadena para cada valor.
   - Si desea permitir o bloquear solicitudes web cuando estas contengan uno de los valores o ambos (`OR`), añada ambos valores a la misma condición de coincidencia de cadena.

   En este ejemplo, seleccione Create.

Paso 5A: Crear una condición regex (opcional)

Una condición de expresión regular es un tipo de condición de coincidencia de cadenas y es similar en el sentido de que identifica las cadenas que desea que AWS WAF Classic busque en una solicitud, como un valor especificado en un encabezado o en una cadena de consulta. La principal diferencia es que se utiliza una expresión regular (regex) para especificar el patrón de cadena que se quiere que busque AWS WAF Classic. En este paso, va a crear una condición de coincidencia de regex. En un paso posterior, especificará si desea permitir o bloquear las solicitudes que contengan las cadenas especificadas.

> **Note**
>
> Para obtener más información acerca de las condiciones de coincidencia de regex, consulte Trabajar con condiciones de coincidencia de regex.

Para crear una condición de coincidencia de regex

1. En la página Create conditions (Crear condiciones), para String match and regex conditions (Condiciones de cadena y expresiones regulares), elija Create condition (Crear condición).
2. En el cuadro de diálogo Create string match condition (Crear condición de coincidencia de cadena), escriba los valores siguientes:

Nombre

Escriba un nombre. El nombre solo puede contener caracteres alfanuméricos (A-Z, a-z, 0-9) o los siguientes caracteres especiales: _-!"#`+*},./.

Tipo

Elija Regex match.

Parte de la solicitud para filtrar en

Elija la parte de la solicitud web que desee que AWS WAF Classic inspeccione en busca de una cadena específica.

En este ejemplo, elija Body.

> **Note**
>
> Si eliges Body como valor de la parte de la solicitud que deseas filtrar, AWS WAF Classic inspecciona solo los primeros 8192 bytes (8 KB), ya que solo CloudFront reenvía los primeros 8192 bytes para su inspección. Para permitir o bloquear solicitudes cuyo cuerpo tenga más de 8192 bytes, puede crear una condición de restricción de tamaño. (AWS WAF Classic obtiene la longitud del cuerpo de los encabezados de las solicitudes). Para obtener más información, consulte Trabajar con condiciones de restricción de tamaño.

Transformación

Para evitar la AWS WAF versión clásica, los atacantes utilizan un formato inusual en las solicitudes web, por ejemplo, añadiendo espacios en blanco o codificando en URL una parte o la totalidad de las solicitudes. Las transformaciones convierten la solicitud web en un formato más próximo al estándar, ya que eliminan los espacios en blanco, descodifican con URL la solicitud o realizan otras operaciones que eliminan gran parte del formato fuera de lo corriente que los atacantes suelen utilizar.

Solo puede especificar un único tipo de transformación de texto.

En este ejemplo, seleccione None.

Regex patterns to match to request

Elija Create regex pattern set.

Nombre del nuevo patrón

Introduzca un nombre y, a continuación, especifique el patrón de expresiones regulares que desea que busque AWS WAF Classic.

A continuación, introduzca la expresión regular I [a@] mAb [a@] dRequest. AWS WAF Classic inspeccionará el `User-Agent` encabezado de las solicitudes web en busca de los valores:

- Soy BadRequest
- IamAB@dRequest
- Yo @mA BadRequest
- I@mAB@dRequest

3. Elija Create pattern set and add filter.
4. Seleccione Crear.

Paso 6: Crear una condición de coincidencia de inyecciones SQL

Una condición de coincidencia de inyección de SQL identifica la parte de las solicitudes web, como un encabezado o una cadena de consulta, que desea que AWS WAF Classic inspeccione en busca de código SQL malicioso. Los atacantes utilizan consultas SQL para extraer datos de su base de datos. En este paso, va a crear una condición de coincidencia de inyección de código SQL. En un paso posterior, especificará si desea permitir o bloquear las solicitudes que parecen contener código SQL malintencionado.

> **Note**
>
> Para obtener más información acerca de las condiciones de coincidencia de cadena, consulte Trabajar con condiciones de coincidencia de inyección de código SQL.

Para crear una condición de coincidencia de inyección de código SQL

1. En la página Create conditions, para SQL injection match conditions, elija Create condition.

2. En el cuadro de diálogo Create SQL injection match condition (Crear condición de coincidencia de inyección SQL), escriba los valores siguientes:

   Nombre

   Escriba un nombre.

   Parte de la solicitud para filtrar en

   Elige la parte de las solicitudes web que quieres que AWS WAF Classic inspeccione para detectar código SQL malintencionado.

   Para este ejemplo, elija Query string.

   > **Note**
   >
   > Si selecciona Body como valor de la parte de la solicitud que desea filtrar, AWS WAF Classic inspecciona solo los primeros 8192 bytes (8 KB), ya que solo CloudFront reenvía los primeros 8192 bytes para su inspección. Para permitir o bloquear solicitudes cuyo cuerpo tenga más de 8192 bytes, puede crear una condición de restricción de tamaño. (AWS WAF Classic obtiene la longitud del cuerpo de los encabezados de las solicitudes). Para obtener más información, consulte Trabajar con condiciones de restricción de tamaño.

   Transformación

   En este ejemplo, seleccione URL decode.

   Los atacantes utilizan un formato inusual, como la codificación de URL, para evitar la AWS WAF versión clásica. La opción Descodificar la URL elimina parte de este formato en la solicitud web antes de que AWS WAF Classic inspeccione la solicitud.

   Solo puede especificar un único tipo de transformación de texto.

3. Seleccione Crear.
4. Elija Siguiente.

Paso 7: (opcional) Crear condiciones adicionales

AWS WAF La versión clásica incluye otras condiciones, entre las que se incluyen las siguientes:

- Condiciones de restricción de tamaño: identifica la parte de las solicitudes web, como un encabezado o una cadena de consulta, cuya longitud desea que AWS WAF Classic compruebe. Para obtener más información, consulte Trabajar con condiciones de restricción de tamaño.
- Condiciones de coincidencia de secuencias de comandos entre sitios: identifica la parte de las solicitudes web, como un encabezado o una cadena de consulta, que desea inspeccionar AWS WAF para detectar scripts maliciosos. Para obtener más información, consulte Trabajar con condiciones de coincidencia de scripting entre sitios.

Si lo desea, puede crear estas condiciones ahora o puede pasar a Paso 8: Crear una regla y agregar condiciones.

Paso 8: Crear una regla y agregar condiciones

Puede crear una regla para especificar las condiciones que desea que AWS WAF Classic busque en las solicitudes web. Si agregas más de una condición a una regla, una solicitud web debe cumplir todas las condiciones de la regla para que la AWS WAF versión clásica permita o bloquee las solicitudes basadas en esa regla.

> **Note**
>
> Para obtener más información acerca de las reglas, consulte Trabajar con reglas.

Para crear una regla y añadir condiciones

1. En la página Create rules, seleccione Create rule.
2. En el cuadro de diálogo Create rule (Crear regla), especifique los valores siguientes:

   Nombre

   Escriba un nombre.

CloudWatch nombre de la métrica

Introduzca un nombre para la CloudWatch métrica que AWS WAF Classic creará y asociará a la regla. El nombre solo puede contener caracteres alfanuméricos (A-Z, a-z y 0-9). No puede contener espacios en blanco.

Tipo de regla

Elija Regular rule (Regla normal) o Rate-based rule (Regla basada en frecuencia). Las reglas basadas en frecuencia son idénticas a las normales, pero también tienen en cuenta el número de solicitudes que proceden de la dirección IP identificada en cualquier período de cinco minutos. Para obtener más información acerca de estos tipos de regla, consulte Cómo funciona AWS WAF Classic. En este ejemplo, seleccione `Regular rule`.

Límite de frecuencia

Para una regla basada en frecuencia, introduzca el número máximo de solicitudes que desea permitir en cualquier periodo de cinco minutos desde una dirección IP que coincida con las condiciones de la regla.

3. Para la primera condición que desea añadir a la regla, especifique la configuración siguiente:

   - Elija si quiere que AWS WAF Classic permita o bloquee las solicitudes en función de si una solicitud web coincide o no con la configuración de la condición.

     En este ejemplo, elija does.

   - Elija el tipo de condición que desea añadir a la regla: una condición de coincidencia de IP, una condición de coincidencia de cadena o una condición de coincidencia de inyección de código SQL.

     En este ejemplo, elija originate from IP addresses in.

   - Elija la condición que desea añadir a la regla.

     En este ejemplo, elija la condición de coincidencia de IP que ha creado en las tareas anteriores.

4. Elija Add condition.
5. Añada la condición de coincidencia geográfica que creó anteriormente. Especifique los siguientes valores:

   - When a request does

- originate from a geographic location in
- Elija su condición de coincidencia geográfica.

6. Elija Add another condition.
7. Añada la condición de coincidencia de cadena que ha creado anteriormente. Especifique los siguientes valores:
   - When a request does
   - match at least one of the filters in the string match condition
   - Elija su condición de coincidencia de cadena.
8. Elija Add condition.
9. Añada la condición de coincidencia de inyección de código SQL que ha creado anteriormente. Especifique los siguientes valores:
   - When a request does
   - match at least one of the filters in the SQL injection match condition
   - Elija su condición de coincidencia de inyección de código SQL.
10. Elija Add condition.
11. Añada la condición de restricción de tamaño que ha creado anteriormente. Especifique los siguientes valores:
    - When a request does
    - match at least one of the filters in the size constraint condition
    - Elija su condición de restricción de tamaño.
12. Si ha creado otras condiciones, como una condición de expresión regular, añádalas de manera similar.
13. Seleccione Crear.
14. En Default action, elija Allow all requests that don't match any rules.
15. Elija Review and create.

Paso 9: Agregar la regla a una ACL web

Cuando añada la regla a una ACL web, debe especificar la configuración siguiente:

- La acción que quieres que AWS WAF Classic lleve a cabo con las solicitudes web que cumplan todas las condiciones de la regla: permitir, bloquear o contar las solicitudes.
- La acción predeterminada para la ACL web. Esta es la acción que quieres que AWS WAF Classic lleve a cabo en las solicitudes web que no cumplan todas las condiciones de la regla: permitir o bloquear las solicitudes.

AWS WAF Classic comienza a bloquear las solicitudes CloudFront web que cumplen las siguientes condiciones (y cualquier otra que hayas añadido):

- El valor del encabezado `User-Agent` es `BadBot`
- (Si creó y añadió la condición regex) El valor de `Body` es cualquiera de las cuatro cadenas que coincida con el patrón `I[a@]mAB[a@]dRequest`
- Las solicitudes provienen de direcciones IP que están entre 192.0.2.0 y 192.0.2.255
- Las solicitudes provienen del país seleccionado en la condición de coincidencia geográfica
- Parece que las solicitudes incluyen código SQL malintencionado en la cadena de consulta

AWS WAF Classic permite responder CloudFront a cualquier solicitud que no cumpla estas tres condiciones.

Paso 10: Eliminar los recursos

Acaba de completar correctamente el tutorial. Para evitar que tu cuenta acumule cargos adicionales en la AWS WAF versión clásica, debes limpiar los objetos AWS WAF clásicos que has creado. O bien puede cambiar la configuración para que coincida con las solicitudes web que realmente desee permitir, bloquear o contar.

> **Note**
>
> AWS normalmente te factura menos de 0,25 USD al día por los recursos que crees durante este tutorial. Cuando haya acabado, le recomendamos que elimine los recursos para evitar incurrir en gastos innecesarios.

Para eliminar los objetos por los que AWS WAF Classic cobra

1. Desasocie su ACL web de su CloudFront distribución:

a. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.

b. Elija el nombre de la ACL web que desea eliminar. Esto abre una página con los detalles de la ACL web en el panel derecho.

c. En el panel de la derecha, en la pestaña Reglas, vaya a la sección Recursos de AWS que utilizan esta ACL web. Para la CloudFront distribución a la que asoció la ACL web, elija la x en la columna Tipo.

2. Elimine las condiciones de la regla:

   a. En el panel de navegación, seleccione Reglas.

   b. Seleccione la regla que ha creado durante el tutorial.

   c. Elija Edit rule.

   d. Seleccione la x que está en el lado derecho de cada encabezado de condición.

   e. Seleccione Actualizar.

3. Elimine la regla de la ACL web y elimine la ACL web:

   a. En el panel de navegación, seleccione Web ACLs (ACL web).

   b. Elija el nombre de ACL web que ha creado durante el tutorial. Esto abre una página con los detalles de la ACL web en el panel derecho.

   c. En la pestaña Rules, elija Edit web ACL.

   d. Seleccione la x situada a la derecha del encabezado de la regla.

   e. Seleccione Actions y, luego, Delete web ACL.

4. Elimine la regla:

   a. En el panel de navegación, seleccione Reglas.

   b. Seleccione la regla que ha creado durante el tutorial.

   c. Elija Eliminar.

   d. En el cuadro de diálogo Delete, vuelva a seleccionar Delete para confirmar la operación.

AWS WAF Classic no cobra por las condiciones, pero si desea completar la limpieza, lleve a cabo el siguiente procedimiento para quitar los filtros de las condiciones y eliminarlas.

Para eliminar filtros y condiciones

1. Elimine el rango de direcciones IP de la condición de coincidencia de IP y elimine la condición de coincidencia de IP:
   a. En el panel de navegación de la consola AWS WAF clásica, elija las direcciones IP.
   b. Seleccione la condición de coincidencia de IP que ha creado durante el tutorial.
   c. Seleccione la casilla de verificación del rango de direcciones IP que ha añadido.
   d. Elija Delete IP address or range (Eliminar dirección IP o rango).
   e. En el panel IP match conditions, elija Delete.
   f. En el cuadro de diálogo Delete, vuelva a seleccionar Delete para confirmar la operación.
2. Elimine el filtro en la condición de coincidencia de inyección de código SQL y elimine la condición de coincidencia de inyección de código SQL:
   a. En el panel de navegación, seleccione SQL injection (Inyección de código SQL).
   b. Seleccione la condición de coincidencia de inyección de código SQL que ha creado durante el tutorial.
   c. Seleccione la casilla de verificación del filtro que ha añadido.
   d. Elija Delete filter (Eliminar filtro).
   e. En el panel SQL injection match conditions, elija Delete.
   f. En el cuadro de diálogo Delete, vuelva a seleccionar Delete para confirmar la operación.
3. Elimine el filtro de la condición de coincidencia de cadena y elimine la condición de coincidencia de la cadena:
   a. En el panel de navegación, elija String and regex matching (Coincidencia de cadenas y regex).
   b. Seleccione la condición de coincidencia de cadena que ha creado durante el tutorial.
   c. Seleccione la casilla de verificación del filtro que ha añadido.
   d. Elija Delete filter (Eliminar filtro).
   e. En el panel String match conditions, elija Delete.
   f. En el cuadro de diálogo Delete, vuelva a seleccionar Delete para confirmar la operación.
4. Si creó alguno, elimine el filtro de la condición de coincidencia de regex y elimine la condición de coincidencia de regex:

a. En el panel de navegación, elija String and regex matching (Coincidencia de cadenas y regex).
b. Elija la condición de coincidencia de regex que ha creado durante el tutorial.
c. Seleccione la casilla de verificación del filtro que ha añadido.
d. Elija Delete filter (Eliminar filtro).
e. En el panel Regex match conditions, elija Delete.
f. En el cuadro de diálogo Delete, vuelva a seleccionar Delete para confirmar la operación.

5. Elimine el filtro de su condición de restricción de tamaño y elimine la condición de restricción de tamaño:

a. En el panel de navegación, elija Size constraints (Restricciones de tamaño).
b. Seleccione la condición de restricción de tamaño que ha creado durante el tutorial.
c. Seleccione la casilla de verificación del filtro que ha añadido.
d. Elija Delete filter (Eliminar filtro).
e. En el panel Size constraint conditions, elija Delete.
f. En el cuadro de diálogo Delete, vuelva a seleccionar Delete para confirmar la operación.

Crear y configurar una lista de control de acceso web (ACL web)

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Una lista de control de acceso web (ACL web) le proporciona un control detallado de las solicitudes web a las que responde su API de Amazon API Gateway, su CloudFront distribución de Amazon o Application Load Balancer. Puede permitir o bloquear los siguientes tipos de solicitudes:

- Proceden de una dirección IP o de un rango de direcciones IP
- Proceden de un país o países específicos

- Contienen una cadena especificada o coinciden con un patrón de expresión regular (regex) en una parte determinada de las solicitudes
- Superan una longitud específica
- Pueden contener código SQL malicioso (conocido como inyección SQL)
- Pueden contener scripts maliciosos (conocidos como scripting entre sitios)

También puede probar cualquier combinación de estas condiciones, o bien bloquear o contar solicitudes web que no solo cumplan las condiciones especificadas, sino que también superen un número determinado de solicitudes en un periodo de cinco minutos.

Para elegir las solicitudes que desea que accedan a su contenido o que desea bloquear, realice las siguientes tareas:

1. Elija la acción por defecto para permitir o bloquear solicitudes web que no coincidan con ninguna de las condiciones que se han especificado. Para obtener más información, consulte Decidir sobre la acción predeterminada para una ACL web.
2. Especifique las condiciones para las que desea permitir o bloquear las solicitudes:
   - Para permitir o bloquear las solicitudes en función de si las solicitudes pueden contener scripts maliciosos, cree condiciones de coincidencia de scripting entre sitios. Para obtener más información, consulte Trabajar con condiciones de coincidencia de scripting entre sitios.
   - Para permitir o bloquear las solicitudes en función de las direcciones IP de las que proceden, cree condiciones de coincidencia de IP. Para obtener más información, consulte Trabajar con condiciones de coincidencia de IP.
   - Para permitir o bloquear las solicitudes en función del país del que proceden, cree condiciones de coincidencia geográfica. Para obtener más información, consulte Trabajar con condiciones de coincidencia geográfica.
   - Para permitir o bloquear las solicitudes en función de si las solicitudes superan una longitud específica, cree condiciones de restricción de tamaño. Para obtener más información, consulte Trabajar con condiciones de restricción de tamaño.
   - Para permitir o bloquear las solicitudes en función de si las solicitudes parecen contener código SQL malicioso, cree condiciones de coincidencia de inyección de código SQL. Para obtener más información, consulte Trabajar con condiciones de coincidencia de inyección de código SQL.

- Para permitir o bloquear las solicitudes en función de las cadenas que aparecen en las solicitudes, cree condiciones de coincidencia de cadena. Para obtener más información, consulte Trabajar con condiciones de coincidencia de cadena.
- Para permitir o bloquear las solicitudes en función de un patrón de expresiones regulares que aparece en las solicitudes, cree condiciones de coincidencia de regex. Para obtener más información, consulte Trabajar con condiciones de coincidencia de regex.

3. Añada las condiciones para una o varias reglas. Si agrega más de una condición a la misma regla, las solicitudes web deben cumplir todas las condiciones para que AWS WAF Classic permita o bloquee las solicitudes en función de la regla. Para obtener más información, consulte Trabajar con reglas. Opcionalmente, puede utilizar una regla basada en frecuencia en lugar de una regla normal para limitar el número de solicitudes desde cualquier dirección IP que cumpla las condiciones.
4. Añada las reglas a una ACL web. Para cada regla, especifique si quiere que AWS WAF Classic permita o bloquee las solicitudes en función de las condiciones que haya agregado a la regla. Si agrega más de una regla a una ACL web, AWS WAF Classic evalúa las reglas en el orden en que aparecen en la ACL web. Para obtener más información, consulte Trabajar con ACL web.

   Cuando se añade una nueva regla o se actualizan las existentes, los cambios pueden tardar en aparecer y en estar activos en las ACL web y en los recursos hasta un minuto.

Temas

Uso de condiciones

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Las condiciones especifican cuándo desea permitir o bloquear las solicitudes.

- Para permitir o bloquear las solicitudes en función de si las solicitudes pueden contener scripts maliciosos, cree condiciones de coincidencia de scripting entre sitios. Para obtener más información, consulte Trabajar con condiciones de coincidencia de scripting entre sitios.
- Para permitir o bloquear las solicitudes en función de las direcciones IP de las que proceden, cree condiciones de coincidencia de IP. Para obtener más información, consulte Trabajar con condiciones de coincidencia de IP.
- Para permitir o bloquear las solicitudes en función del país del que proceden, cree condiciones de coincidencia geográfica. Para obtener más información, consulte Trabajar con condiciones de coincidencia geográfica.
- Para permitir o bloquear las solicitudes en función de si las solicitudes superan una longitud específica, cree condiciones de restricción de tamaño. Para obtener más información, consulte Trabajar con condiciones de restricción de tamaño.
- Para permitir o bloquear las solicitudes en función de si las solicitudes parecen contener código SQL malicioso, cree condiciones de coincidencia de inyección de código SQL. Para obtener más información, consulte Trabajar con condiciones de coincidencia de inyección de código SQL.
- Para permitir o bloquear las solicitudes en función de las cadenas que aparecen en las solicitudes, cree condiciones de coincidencia de cadena. Para obtener más información, consulte Trabajar con condiciones de coincidencia de cadena.
- Para permitir o bloquear las solicitudes en función de un patrón de expresiones regulares que aparece en las solicitudes, cree condiciones de coincidencia de regex. Para obtener más información, consulte Trabajar con condiciones de coincidencia de regex.

Temas

Trabajar con condiciones de coincidencia de scripting entre sitios

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Los atacantes a veces insertan scripts en solicitudes web para aprovechar las vulnerabilidades de las aplicaciones web. Puede crear una o más condiciones de coincidencia de secuencias de comandos entre sitios para identificar las partes de las solicitudes web, como el URI o la cadena de consulta, que desea que AWS WAF Classic inspeccione para detectar posibles secuencias de comandos maliciosas. Más adelante, cuando cree una ACL web, puede especificar si desea permitir o bloquear las solicitudes que parecen contener scripts maliciosos.

Temas

Crear condiciones de coincidencia de scripting entre sitios

Cuando se crean condiciones de coincidencia de scripting entre sitios, se especifican filtros. Los filtros indican la parte de las solicitudes web que desea que AWS WAF Classic inspeccione para detectar scripts maliciosos, como el URI o la cadena de consulta. Puede añadir más de un filtro a una condición de coincidencia de scripting entre sitios o bien puede crear una condición independiente para cada filtro. Así es como afecta cada configuración al comportamiento de la AWS WAF versión clásica:

- Más de un filtro por condición de coincidencia de secuencias de comandos entre sitios (recomendado): cuando se agrega una condición de coincidencia de secuencias de comandos entre sitios que contiene varios filtros a una regla y se agrega la regla a una ACL web, una solicitud web debe coincidir solo con uno de los filtros de la condición de coincidencia de secuencias de

comandos entre sitios para que AWS WAF Classic permita o bloquee la solicitud en función de esa condición.

Por ejemplo, suponga que crea una condición de coincidencia de scripting entre sitios y la condición contiene dos filtros. Un filtro indica a AWS WAF Classic que inspeccione el URI en busca de scripts maliciosos y el otro indica a AWS WAF Classic que inspeccione la cadena de consulta. AWS WAF Classic permite o bloquea las solicitudes si parecen contener scripts maliciosos en el URI o en la cadena de consulta.

- Un filtro por condición de coincidencia de secuencias de comandos entre sitios: al añadir las distintas condiciones de coincidencia de secuencias de comandos entre sitios a una regla y añadir la regla a una ACL web, las solicitudes web deben cumplir todas las condiciones para que la AWS WAF versión clásica permita o bloquee las solicitudes en función de esas condiciones.

  Supongamos que crea dos condiciones y que cada condición contiene uno de los dos filtros del ejemplo anterior. Al añadir ambas condiciones a la misma regla y añadir la regla a una ACL web, AWS WAF Classic solo permite o bloquea las solicitudes cuando tanto el URI como la cadena de consulta parecen contener scripts maliciosos.

> **Note**
>
> Al añadir una condición de coincidencia de secuencias de comandos entre sitios a una regla, también puede configurar la AWS WAF versión clásica para que permita o bloquee las solicitudes web que no parezcan contener scripts maliciosos.

Para crear una condición de coincidencia de scripting entre sitios

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, seleccione Cross-site scripting.
3. Elija Create condition.
4. Especifique la configuración de filtro aplicable. Para obtener más información, consulte Valores que se especifican al crear o editar condiciones de coincidencia de scripting entre sitios.
5. Elija Add another filter.

6. Si desea añadir otro filtro, repita los pasos 4 y 5.
7. Cuando haya acabado de añadir filtros, seleccione Create.

Valores que se especifican al crear o editar condiciones de coincidencia de scripting entre sitios

Al crear o actualizar una condición de coincidencia de scripting entre sitios, debe especificar los siguientes valores:

Nombre

Es el nombre de la condición de coincidencia de scripting entre sitios.

El nombre solo puede contener los caracteres A-Z, a-z, 0-9 y los caracteres especiales: _-!"#` +*},./ . No se puede cambiar el nombre de una condición después de crearla.

Parte de la solicitud para filtrar en

Elige la parte de cada solicitud web que quieres que AWS WAF Classic inspeccione para detectar scripts maliciosos:

Encabezado

Un encabezado de solicitud específico, por ejemplo, el encabezado `User-Agent` o `Referer`. Si elige Header, indique el nombre del encabezado en el campo Header.

Método HTTP

El método HTTP indica el tipo de operación que la solicitud pide al origen que lleve a cabo. CloudFront admite los siguientes métodos: `DELETEGET`,`HEAD`, `OPTIONSPATCH`,`POST`, y`PUT`.

Cadena de consulta

Es la parte de una URL que aparece después de un carácter `?`, si hay alguno.

> **Note**
>
> En situaciones de coincidencia de secuencias de comandos entre sitios, recomendamos elegir All query parameters (values only) (Todos los parámetros de consulta [solo valores]) en vez de Query string (Cadena de consulta) para Part of the request to filter on (Parte de la consulta que se va a filtrar).

URI

La ruta del URI de la solicitud, que identifica el recurso, por ejemplo, `/images/daily-ad.jpg`. Esto no incluye la cadena de consulta ni los componentes del fragmento del URI. Para obtener información, consulte Identificador uniforme de recursos (URI): sintaxis genérica.

A menos que se especifique una transformación, el URI no se normaliza y se inspecciona tal y como lo AWS recibe del cliente como parte de la solicitud. Una transformación reformateará el URI según se especifique.

Cuerpo

Es la parte de una solicitud que contiene los datos adicionales que desea enviar a su servidor web como cuerpo de la solicitud HTTP, por ejemplo, los datos de un formulario.

> **Note**
>
> Si, por el contrario, elige Cuerpo para el valor de Parte de la consulta que se va a filtrar, AWS WAF Classic solo inspeccionará los primeros 8192 bytes (8 KB). Para permitir o bloquear solicitudes cuyo cuerpo tenga más de 8192 bytes, puede crear una condición de restricción de tamaño. (AWS WAF Classic obtiene la longitud del cuerpo de los encabezados de las solicitudes). Para obtener más información, consulte Trabajar con condiciones de restricción de tamaño.

Parámetro de consulta único (solo valor)

Cualquier parámetro que haya definido como parte de la cadena de consulta. Por ejemplo, si la URL es «www.xyz.com? UserName =abc& SalesRegion =seattle», puede añadir un filtro al parámetro o. UserNameSalesRegion

Si elige Single query parameter (value only) (Parámetro de consulta único [solo valor]), también debe especificar un Query parameter name (Nombre de parámetro de consulta). Este es el parámetro de la cadena de consulta que inspeccionará, como o. UserNameSalesRegion La longitud máxima del Query parameter name (Nombre de parámetro de consulta) es de 30 caracteres. Query parameter name (Nombre de parámetro de consulta) no distingue entre mayúsculas y minúsculas. Por ejemplo, si lo especificas UserNamecomo nombre del parámetro de consulta, coincidirá con todas las variantes UserName, como username y userName.

Todos los parámetros de consulta (solo valores)

Al igual que con el parámetro de consulta único (solo valores), pero en lugar de inspeccionar los valores de un solo parámetro, AWS WAF Classic inspecciona todos los valores de los parámetros de la cadena de consulta para detectar posibles scripts maliciosos. Por ejemplo, si la URL es «www.xyz.com? UserName =abc& SalesRegion =seattle» y selecciona Todos los parámetros de la consulta (solo valores), AWS WAF Classic activará una coincidencia si el valor o contiene posibles scripts maliciosos. UserNameSalesRegion

Encabezado

Si selecciona Encabezado como parte de la solicitud por la que desea filtrar, elija un encabezado de la lista de encabezados más comunes o introduzca el nombre del encabezado que desee que Classic inspeccione para detectar scripts maliciosos. AWS WAF

Transformación

Una transformación reformatea una solicitud web antes de que AWS WAF Classic la inspeccione. Esto elimina algunos de los formatos poco habituales que los atacantes utilizan en las solicitudes web para evitar AWS WAF la versión clásica.

Solo puede especificar un único tipo de transformación de texto.

Las transformaciones pueden realizar las siguientes operaciones:

Ninguna

AWS WAF Classic no realiza ninguna transformación de texto en la solicitud web antes de inspeccionarla para comprobar si coincide con la cadena de Value.

Cambiar a minúsculas

AWS WAF Classic convierte las letras mayúsculas (A-Z) en minúsculas (a-z).

Descodificar en HTML

AWS WAF La versión clásica reemplaza los caracteres codificados en HTML por caracteres no codificados:

- Sustituye `"` por &
- Sustituye ` ` por un espacio de no separación
- Sustituye `<` por <
- Sustituye `>` por >

- Sustituye los caracteres representados con formato hexadecimal, `&#xhhhh;`, por los caracteres correspondientes
- Sustituye los caracteres representados con formato decimal, `&#nnnn;`, por los caracteres correspondientes

Normalizar espacios en blanco

AWS WAF La versión clásica reemplaza los siguientes caracteres por un carácter de espacio (32 decimales):

- \f, salto de página, 12 decimales
- \t, pestaña, 9 decimales
- \n, línea nueva, 10 decimales
- \r, salto de línea, 13 decimales
- \v, pestaña vertical, 11 decimales
- espacio de no separación, 160 decimales

Además, esta opción sustituye varios espacios por un espacio.

Simplificar la línea de comandos

Para las solicitudes que contienen los comandos de línea de comandos del sistema operativo, utilice esta opción para realizar las siguientes transformaciones:

- Eliminar los siguientes caracteres: \ " ' ^
- Eliminar los espacios delante de los siguientes caracteres: / (
- Sustituir los siguientes caracteres por un espacio: , ;
- Sustituir varios espacios por un espacio
- Convertir las mayúsculas (A-Z) en minúsculas (a-z)

Descodificar la URL

Descodifique una solicitud de URL codificada.

Agregar y eliminar filtros en una condición de coincidencia de scripting entre sitios

Puede añadir o eliminar filtros en una condición de coincidencia de scripting entre sitios. Para cambiar un filtro, añada uno nuevo y elimine el viejo.

Para añadir o eliminar filtros en una condición de coincidencia de scripting entre sitios

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, seleccione Cross-site scripting.
3. Elija la condición para la que desea añadir o eliminar filtros.
4. Para añadir filtros, siga los siguientes pasos:

   a. Elija Add filter (Agregar filtro).

   b. Especifique la configuración de filtro aplicable. Para obtener más información, consulte Valores que se especifican al crear o editar condiciones de coincidencia de scripting entre sitios.

   c. Elija Add (Agregar).
5. Para eliminar filtros, siga los siguientes pasos:

   a. Seleccione el filtro que desea eliminar.

   b. Elija Delete filter (Eliminar filtro).

Eliminar condiciones de coincidencia de scripting entre sitios

Si desea eliminar una condición de coincidencia de scripting entre sitios, primero debe eliminar todos los filtros de la condición y borrar la condición de todas las reglas que la utilizan, tal y como se describe en el siguiente procedimiento.

Para eliminar una condición de coincidencia de scripting entre sitios

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, seleccione Cross-site scripting.
3. En el panel Cross-site scripting match conditions (Condiciones de coincidencia de scripting entre sitios), elija la condición de coincidencia de scripting entre sitios que desea eliminar.
4. En el panel de la derecha, elija la pestaña Associated rules (Reglas asociadas).

Si la lista de reglas que utilizan esta condición de coincidencia de scripting entre sitios está vacía, vaya al paso 6. Si la lista contiene alguna regla, anótela y continúe con el paso 5.

5. Para eliminar la condición de coincidencia de scripting entre sitios de las reglas que la utilizan, siga los siguientes pasos:

   a. En el panel de navegación, seleccione Rules (Reglas).

   b. Elija el nombre de una regla que utilice la condición de coincidencia de scripting entre sitios que desea eliminar.

   c. En el panel de la derecha, seleccione la condición de coincidencia de scripting entre sitios que desea eliminar de la regla y elija Remove selected condition (Eliminar condición seleccionada).

   d. Repita los pasos b y c para todas las demás reglas que utilizan la condición de coincidencia de scripting entre sitios que desea eliminar.

   e. En el panel de navegación, seleccione Cross-site scripting.

   f. En el panel Cross-site scripting match conditions (Condiciones de coincidencia de scripting entre sitios), elija la condición de coincidencia de scripting entre sitios que desea eliminar.

6. Elija Delete (Eliminar) para eliminar la condición seleccionada.

Trabajar con condiciones de coincidencia de IP

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Si desea permitir o bloquear solicitudes web en función de las direcciones IP de las que proceden las solicitudes, cree una o más condiciones de coincidencia de IP. Una condición de coincidencia enumera hasta 10 000 direcciones IP o rangos de direcciones IP de las que proceden sus solicitudes. Más adelante, cuando cree una ACL web, puede especificar si desea permitir o bloquear las solicitudes de dichas direcciones IP.

Temas

Creación de una condición de coincidencia de IP

Si desea permitir algunas solicitudes web y bloquear otras en función de las direcciones IP de donde proceden las solicitudes, cree una condición de coincidencia de IP para las direcciones IP que desea permitir y otra condición de coincidencia de IP para las direcciones IP que desea bloquear.

> **Note**
>
> Al añadir una condición de coincidencia de IP a una regla, también puede configurar la AWS WAF versión clásica para permitir o bloquear las solicitudes web que no se originen en las direcciones IP que especifique en la condición.

Para crear una condición de coincidencia de IP

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, seleccione IP addresses (Direcciones IP).
3. Elija Create condition.
4. Escriba un nombre en el campo Name (Nombre) .

   El nombre solo puede contener caracteres alfanuméricos (A-Z, a-z, 0-9) o los siguientes caracteres especiales: _-!"#`+*},./. No se puede cambiar el nombre de una condición después de crearla.
5. Seleccione la versión IP correcta e indique una dirección IP o un rango de direcciones IP mediante la notación CIDR. Estos son algunos ejemplos:

   - Para especificar la dirección IPv4 192.0.2.44, escriba 192.0.2.44/32.
   - Para especificar la dirección IPv6 0:0:0:0:0:ffff:c000:22c, escriba 0:0:0:0:0:ffff:c000:22c/128.

- Para especificar el rango de direcciones IPv4 de 192.0.2.0 a 192.0.2.255, escriba 192.0.2.0/24.
- Para especificar el rango de direcciones IPv6 de 2620:0:2d0:200:0:0:0:0 a 2620:0:2d0:200:ffff:ffff:ffff:ffff, introduzca 2620:0:2d0:200::/64.

AWS WAF Classic admite rangos de direcciones IPv4: /8 y cualquier rango entre /16 y /32. AWS WAF Classic admite los rangos de direcciones IPv6: /24, /32, /48, /56, /64 y /128. Para obtener más información acerca de la notación CIDR, consulte la entrada de la Wikipedia Classless Inter-Domain Routing.

6. Elija Add another IP address or range (Agregar otra dirección IP u otro rango).
7. Si desea añadir otra dirección IP u otro rango, repita los pasos 5 y 6.
8. Cuando termine de agregar valores, elija Create IP match condition (Crear condición de coincidencia de IP).

Editar condiciones de coincidencia de IP

Puede añadir un rango de direcciones IP a una condición de coincidencia de IP o eliminar un rango. Para cambiar un rango, añada uno nuevo y elimine el antiguo.

Para editar una condición de coincidencia de IP

1. Inicie sesión en la consola y ábrala en https://console.aws.amazon.com/wafv2/. AWS Management ConsoleAWS WAF

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, seleccione IP addresses (Direcciones IP).
3. En el panel IP match conditions (Condiciones de coincidencia de IP), elija la condición de coincidencia de IP que desea editar.
4. Para añadir un rango de direcciones IP:

   a. En el panel derecho, elija Add IP address or range (Agregar otra dirección IP u otro rango).

   b. Seleccione la versión IP correcta y escriba un rango de direcciones IP mediante la notación CIDR. Estos son algunos ejemplos:

      - Para especificar la dirección IPv4 192.0.2.44, escriba 192.0.2.44/32.

- Para especificar la dirección IPv6 0:0:0:0:0:ffff:c000:22c, escriba 0:0:0:0:0:ffff:c000:22c/128.
- Para especificar el rango de direcciones IPv4 de 192.0.2.0 a 192.0.2.255, escriba 192.0.2.0/24.
- Para especificar el rango de direcciones IPv6 de 2620:0:2d0:200:0:0:0:0 a 2620:0:2d0:200:ffff:ffff:ffff:ffff, introduzca 2620:0:2d0:200::/64.

AWS WAF Classic admite rangos de direcciones IPv4: /8 y cualquier rango entre /16 y /32. AWS WAF Classic admite los rangos de direcciones IPv6: /24, /32, /48, /56, /64 y /128. Para obtener más información acerca de la notación CIDR, consulte la entrada de la Wikipedia Classless Inter-Domain Routing.

c. Para agregar más direcciones IP, elija Add another IP address (Agregar otra dirección IP) y escriba el valor.

d. Elija Añadir.

5. Para eliminar una dirección IP o un rango:

a. En el panel de la derecha, seleccione los valores que desea eliminar.

b. Elija Delete IP address or range (Eliminar dirección IP o rango).

Eliminar condiciones de coincidencia de IP

Si desea eliminar una condición de coincidencia de IP, primero debe eliminar todas las direcciones IP y todos los rangos de la condición y borrar la condición de todas las reglas que la utilizan, tal y como se describe en el siguiente procedimiento.

Para eliminar una condición de coincidencia de IP

1. Inicie sesión en la consola y ábrala en https://console.aws.amazon.com/wafv2/. AWS Management ConsoleAWS WAF

Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.

2. En el panel de navegación, seleccione IP addresses (Direcciones IP).
3. En el panel IP match conditions, elija la condición de coincidencia de IP que desea eliminar.
4. En el panel de la derecha, elija la pestaña Rules.

Si la lista de reglas que utilizan la condición de coincidencia de IP está vacía, vaya al paso 6. Si la lista contiene alguna regla, anótela y continúe con el paso 5.

5. Para eliminar la condición de coincidencia de IP de las reglas que la utilizan, siga los siguientes pasos:

   a. En el panel de navegación, seleccione Reglas.

   b. Elija el nombre de una regla que utilice la condición de coincidencia de IP que desea eliminar.

   c. En el panel de la derecha, seleccione la condición de coincidencia de IP que desea eliminar de la regla y elija Remove selected condition (Eliminar condición seleccionada).

   d. Repita los pasos b y c para todas las demás reglas que utilizan la condición de coincidencia de IP que desea eliminar.

   e. En el panel de navegación, seleccione IP match conditions.

   f. En el panel IP match conditions, elija la condición de coincidencia de IP que desea eliminar.

6. Elija Delete (Eliminar) para eliminar la condición seleccionada.

Trabajar con condiciones de coincidencia geográfica

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Si desea permitir o bloquear solicitudes web en función del país del que proceden las solicitudes, cree una o más condiciones de coincidencia geográfica. Una condición de coincidencia geográfica enumera los países de los que provienen las solicitudes. Más adelante, cuando cree una ACL web, puede especificar si desea permitir o bloquear las solicitudes procedentes de dichos países.

Puede utilizar las condiciones de coincidencia geográfica con otras condiciones o reglas AWS WAF clásicas para crear filtros sofisticados. Por ejemplo, si desea bloquear determinados países, pero seguir permitiendo direcciones IP específicas de dichos países, puede crear una regla que contenga

una condición de coincidencia geográfica y una condición de coincidencia de IP. Configure la regla para bloquear las solicitudes que provengan de ese país y no coincidan con las direcciones IP aprobadas. Otro ejemplo: si desea dar prioridad a los recursos para los usuarios de un determinado país, podría incluir una condición de coincidencia geográfica con dos reglas diferente basadas en frecuencia. Establezca un límite de frecuencia mayor para los usuarios del país preferido y un límite de frecuencia menor para todos los demás usuarios.

> **Note**
>
> Si utilizas la función de restricción CloudFront geográfica para impedir que un país acceda a tu contenido, cualquier solicitud de ese país quedará bloqueada y no se reenviará a la AWS WAF versión clásica. Por lo tanto, si quieres permitir o bloquear las solicitudes en función de la ubicación geográfica y otras condiciones AWS WAF clásicas, no debes usar la función de restricción CloudFront geográfica. En su lugar, debes usar una condición de coincidencia geográfica AWS WAF clásica.

Temas

- Crear una condición de coincidencia geográfica
- Editar condiciones de coincidencia geográfica
- Eliminar condiciones de coincidencia geográfica

Crear una condición de coincidencia geográfica

Si desea permitir algunas solicitudes web y bloquear otras en función de los países de donde proceden las solicitudes, cree una condición de coincidencia geográfica para los países que desea permitir y otra condición de coincidencia geográfica para los países que desea bloquear.

> **Note**
>
> Al añadir una condición de coincidencia geográfica a una regla, también puede configurar la AWS WAF versión clásica para permitir o bloquear las solicitudes web que no se originen en el país que especifique en la condición.

Para crear una condición de coincidencia geográfica

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, elija Geo match.
3. Elija Create condition.
4. Escriba un nombre en el campo Name (Nombre) .

   El nombre solo puede contener caracteres alfanuméricos (A-Z, a-z, 0-9) o los siguientes caracteres especiales: _-!"#`+*},./. No se puede cambiar el nombre de una condición después de crearla.
5. Elija una región en Region.
6. Elija un valor en Location type (Tipo de ubicación) y un país. El valor de Location type (Tipo de ubicación), actualmente, solo puede ser Country (País).
7. Elija Add location (Agregar ubicación).
8. Seleccione Crear.

Editar condiciones de coincidencia geográfica

Puede añadir países o eliminar países de su condición de coincidencia geográfica.

Para editar una condición de coincidencia geográfica

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, elija Geo match.
3. En el panel Condiciones de coincidencia geográfica, elija la condición de coincidencia geográfica que desea editar.
4. Para añadir un país:

   a. En el panel derecho, elija Add filter (Agregar filtro).
   b. Elija un valor en Location type (Tipo de ubicación) y un país. El valor de Location type (Tipo de ubicación), actualmente, solo puede ser Country (País).

c. Elija Añadir.

5. Para eliminar un país:

   a. En el panel de la derecha, seleccione los valores que desea eliminar.

   b. Elija Delete filter (Eliminar filtro).

Eliminar condiciones de coincidencia geográfica

Si desea eliminar una condición de coincidencia geográfica, primero debe quitar todos los países de la condición y quitar la condición de todas las reglas que la utilizan, tal y como se describe en el siguiente procedimiento.

Para eliminar una condición de coincidencia geográfica

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.

2. Quite la condición de coincidencia geográfica de las reglas que la utilizan:

   a. En el panel de navegación, seleccione Reglas.

   b. Elija el nombre de una regla que utilice la condición de coincidencia geográfica que desea eliminar.

   c. En el panel de la derecha, elija Edit rule (Editar regla).

   d. Elija la X situada al lado de la condición que desea eliminar.

   e. Seleccione Actualizar.

   f. Repita estos pasos para todas las demás reglas que utilizan la condición de coincidencia geográfica que desea eliminar.

3. Quite los filtros de la condición que desea eliminar:

   a. En el panel de navegación, elija Geo match.

   b. Elija el nombre de la condición de coincidencia geográfica que desea eliminar.

   c. En el panel de la derecha, elija la casilla de verificación situada junto a Filter para seleccionar todos los filtros.

   d. Elija Delete filter (Eliminar filtro).

4. En el panel de navegación, elija Geo match.

5. En el panel Geo match conditions, elija la condición de coincidencia geográfica que desea eliminar.
6. Elija Delete (Eliminar) para eliminar la condición seleccionada.

Trabajar con condiciones de restricción de tamaño

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Si desea permitir o bloquear solicitudes web en función de la longitud de determinadas partes de las solicitudes, cree una o varias condiciones de restricción de tamaño. Una condición de restricción de tamaño identifica la parte de las solicitudes web que desea que examine AWS WAF Classic, el número de bytes que desea que busque AWS WAF Classic y un operador, como mayor que (>) o menor que (<). Por ejemplo, puede utilizar una condición de restricción de tamaño para buscar las cadenas de consulta que tengan más de 100 bytes. Más adelante, cuando cree una ACL web, puede especificar si desea permitir o bloquear las solicitudes según dicha configuración.

Tenga en cuenta que si configura AWS WAF Classic para inspeccionar el cuerpo de la solicitud, por ejemplo, buscando en el cuerpo una cadena específica, AWS WAF Classic inspecciona solo los primeros 8192 bytes (8 KB). Si el cuerpo de la solicitud para sus solicitudes web nunca va a superar los 8 192 bytes, puede crear una condición de restricción de tamaño y bloquear las solicitudes que tengan un cuerpo de la solicitud que supere los 8 192 bytes.

Temas

- Crear condiciones de restricción de tamaño
- Valores que se especifican al crear o editar condiciones de restricción de tamaño
- Agregar y eliminar filtros en una condición de restricción de tamaño
- Eliminar condiciones de restricción de tamaño

Crear condiciones de restricción de tamaño

Al crear condiciones de restricción de tamaño, se especifican filtros que identifican la parte de las solicitudes web cuya longitud se desea que AWS WAF Classic evalúe. Puede añadir más de un filtro a una condición de restricción de tamaño o puede crear una condición independiente para cada filtro. Así es como afecta cada configuración al comportamiento de la AWS WAF versión clásica:

- Un filtro por condición de restricción de tamaño: al añadir las distintas condiciones de restricción de tamaño a una regla y añadir la regla a una ACL web, las solicitudes web deben cumplir todas las condiciones para que AWS WAF Classic permita o bloquee las solicitudes en función de esas condiciones.

  Por ejemplo, suponga que crea dos condiciones. Una coincide con solicitudes web cuyas cadenas de consulta superan los 100 bytes. La otra coincide con las solicitudes web cuyo cuerpo de la solicitud es superior a 1024 bytes. Al añadir ambas condiciones a la misma regla y añadir la regla a una ACL web, la AWS WAF versión clásica solo permite o bloquea las solicitudes cuando se cumplen ambas condiciones.
- Más de un filtro por condición de restricción de tamaño: cuando se agrega una condición de restricción de tamaño que contiene varios filtros a una regla y se agrega la regla a una ACL web, la solicitud web solo necesita coincidir con uno de los filtros de la condición de restricción de tamaño para que AWS WAF Classic permita o bloquee la solicitud en función de esa condición.

  Supongamos que crea una condición en lugar de dos y que la única condición contiene los mismos dos filtros que en el ejemplo anterior. AWS WAF Classic permite o bloquea las solicitudes si la cadena de consulta es superior a 100 bytes o el cuerpo de la solicitud es superior a 1024 bytes.

> **Note**
>
> Al añadir una condición de restricción de tamaño a una regla, también puede configurar la AWS WAF versión clásica para permitir o bloquear las solicitudes web que no coincidan con los valores de la condición.

Para crear una condición de restricción de tamaño

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.

2. En el panel de navegación, elija Size constraints (Restricciones de tamaño).
3. Elija Create condition.
4. Especifique la configuración de filtro aplicable. Para obtener más información, consulte Valores que se especifican al crear o editar condiciones de restricción de tamaño.
5. Elija Add another filter.
6. Si desea añadir otro filtro, repita los pasos 4 y 5.
7. Cuando termine de agregar filtros, elija Create size constraint condition (Crear condición de restricción de tamaño).

Valores que se especifican al crear o editar condiciones de restricción de tamaño

Al crear o actualizar una condición de restricción de tamaño, debe especificar los siguientes valores:

Nombre

Escriba un nombre para la condición de restricción de tamaño.

El nombre solo puede contener caracteres alfanuméricos (A-Z, a-z, 0-9) o los siguientes caracteres especiales: _-!"#`+*},./. No se puede cambiar el nombre de una condición después de crearla.

Parte de la solicitud para filtrar en

Elija la parte de cada solicitud web cuya longitud desee que AWS WAF Classic evalúe:

Encabezado

Un encabezado de solicitud específico, por ejemplo, el encabezado `User-Agent` o `Referer`. Si elige Header, indique el nombre del encabezado en el campo Header.

Método HTTP

El método HTTP indica el tipo de operación que la solicitud pide al origen que lleve a cabo. CloudFront admite los siguientes métodos: `DELETEGET`,`HEAD`, `OPTIONSPATCH`,`POST`, y`PUT`.

Cadena de consulta

Es la parte de una URL que aparece después de un carácter `?`, si hay alguno.

URI

La ruta del URI de la solicitud, que identifica el recurso, por ejemplo, `/images/daily-ad.jpg`. Esto no incluye la cadena de consulta ni los componentes del fragmento del URI. Para obtener información, consulte Identificador uniforme de recursos (URI): sintaxis genérica.

A menos que se especifique una transformación, el URI no se normaliza y se inspecciona tal y como lo AWS recibe del cliente como parte de la solicitud. Una transformación reformateará el URI según se especifique.

Cuerpo

Es la parte de una solicitud que contiene los datos adicionales que desea enviar a su servidor web como cuerpo de la solicitud HTTP, por ejemplo, los datos de un formulario.

Parámetro de consulta único (solo valor)

Cualquier parámetro que haya definido como parte de la cadena de consulta. Por ejemplo, si la URL es «www.xyz.com? UserName =abc& SalesRegion =seattle», puede añadir un filtro al parámetro o. UserNameSalesRegion

Si elige Single query parameter (value only) (Parámetro de consulta único [solo valor]), también debe especificar un Query parameter name (Nombre de parámetro de consulta). Este es el parámetro de la cadena de consulta que inspeccionará, por ejemplo. UserName La longitud máxima del Query parameter name (Nombre de parámetro de consulta) es de 30 caracteres. Query parameter name (Nombre de parámetro de consulta) no distingue entre mayúsculas y minúsculas. Por ejemplo, si lo especificas UserNamecomo nombre del parámetro de consulta, coincidirá con todas las variantes UserName, como username y userName.

Todos los parámetros de consulta (solo valores)

Similar al parámetro de consulta único (solo valor), pero en lugar de inspeccionar el valor de un solo parámetro, AWS WAF Classic inspecciona los valores de todos los parámetros de la cadena de consulta para comprobar la restricción de tamaño. Por ejemplo, si la dirección URL es «www.xyz.com? UserName =abc& SalesRegion =seattle» y selecciona Todos los parámetros de la consulta (solo valores), AWS WAF Classic activará una coincidencia del valor si alguno de los parámetros de consulta supera o supera el tamaño especificado. UserNameSalesRegion

Encabezado (solo cuando "Parte de la solicitud para filtrar en" es "Encabezado")

Si seleccionó Encabezado como parte de la solicitud para filtrar, elija un encabezado de la lista de encabezados comunes o escriba el nombre del encabezado cuya longitud desee que Classic evalúe. AWS WAF

Operador de comparación

Elige cómo quieres que AWS WAF Classic evalúe la longitud de la cadena de consulta en las solicitudes web con respecto al valor que especifiques en Size.

Por ejemplo, si elige Es mayor que para el operador de comparación y escribe 100 para el tamaño, AWS WAF Classic evalúa las solicitudes web para una cadena de consulta de más de 100 bytes.

Tamaño

Introduzca la longitud, en bytes, que desee que AWS WAF Classic observe en las cadenas de consulta.

> **Note**
>
> Si elige URI para el valor de Part of the request to filter on (Parte de la consulta que se va a filtrar), la / del URI se cuenta como un carácter. Por ejemplo, el `/logo.jpg` de la ruta del URI tiene nueve caracteres.

Transformación

Una transformación reformatea una solicitud web antes de que AWS WAF Classic evalúe la longitud de la parte especificada de la solicitud. Esto elimina algunos de los formatos poco habituales que los atacantes utilizan en las solicitudes web para evitar AWS WAF la versión clásica.

> **Note**
>
> Si seleccionas el cuerpo como parte de la solicitud que deseas filtrar, no podrás configurar AWS WAF Classic para que lleve a cabo una transformación, ya que solo se reenvían los primeros 8192 bytes para su inspección. Sin embargo, puede filtrar el tráfico en función del tamaño del cuerpo de la solicitud HTTP y especificar una transformación

de Ninguna. (AWS WAF Classic obtiene la longitud del cuerpo de los encabezados de las solicitudes).

Solo puede especificar un único tipo de transformación de texto.

Las transformaciones pueden realizar las siguientes operaciones:

Ninguna

AWS WAF Classic no realiza ninguna transformación de texto en la solicitud web antes de comprobar la longitud.

Cambiar a minúsculas

AWS WAF Classic convierte las letras mayúsculas (A-Z) en minúsculas (a-z).

Descodificar en HTML

AWS WAF La versión clásica reemplaza los caracteres codificados en HTML por caracteres no codificados:

- Sustituye `"` por &
- Sustituye ` ` por un espacio de no separación
- Sustituye `<` por <
- Sustituye `>` por >
- Sustituye los caracteres representados con formato hexadecimal, `&#xhhhh;`, por los caracteres correspondientes
- Sustituye los caracteres representados con formato decimal, `&#nnnn;`, por los caracteres correspondientes

Normalizar espacios en blanco

AWS WAF La versión clásica reemplaza los siguientes caracteres por un carácter de espacio (32 decimales):

- \f, salto de página, 12 decimales
- \t, pestaña, 9 decimales
- \n, línea nueva, 10 decimales
- \r, salto de línea, 13 decimales
- \v, pestaña vertical, 11 decimales
- espacio de no separación, 160 decimales

Además, esta opción sustituye varios espacios por un espacio.

Simplificar la línea de comandos

Para las solicitudes que contienen los comandos de línea de comandos del sistema operativo, utilice esta opción para realizar las siguientes transformaciones:

- Eliminar los siguientes caracteres: \ " ' ^
- Eliminar los espacios delante de los siguientes caracteres: / (
- Sustituir los siguientes caracteres por un espacio: , ;
- Sustituir varios espacios por un espacio
- Convertir las mayúsculas (A-Z) en minúsculas (a-z)

Descodificar la URL

Descodifique una solicitud de URL codificada.

Agregar y eliminar filtros en una condición de restricción de tamaño

Puede añadir o eliminar filtros en una condición de restricción de tamaño. Para cambiar un filtro, añada uno nuevo y elimine el viejo.

Para añadir o eliminar filtros en una condición de restricción de tamaño

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, elija Size constraint (Restricción de tamaño).
3. Elija la condición para la que desea añadir o eliminar filtros.
4. Para añadir filtros, siga los siguientes pasos:

   a. Elija Add filter (Agregar filtro).

   b. Especifique la configuración de filtro aplicable. Para obtener más información, consulte Valores que se especifican al crear o editar condiciones de restricción de tamaño.

   c. Elija Add (Agregar).
5. Para eliminar filtros, siga los siguientes pasos:

   a. Seleccione el filtro que desea eliminar.

b. Elija Delete filter (Eliminar filtro).

Eliminar condiciones de restricción de tamaño

Si desea eliminar una condición de restricción de tamaño, primero debe eliminar todos los filtros de la condición y borrar la condición de todas las reglas que la utilizan, tal y como se describe en el siguiente procedimiento.

Para eliminar una condición de restricción de tamaño

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, elija Size constraints (Restricciones de tamaño).
3. En el panel Size constraint conditions (Condiciones de restricción de tamaño), elija la condición de restricción de tamaño que desea eliminar.
4. En el panel de la derecha, elija la pestaña Associated rules (Reglas asociadas).

   Si la lista de reglas que utiliza esta condición de restricción de tamaño está vacía, vaya al paso 6. Si la lista contiene alguna regla, anótela y continúe con el paso 5.
5. Para eliminar la condición de restricción de tamaño de las reglas que la utilizan, siga los siguientes pasos:

   a. En el panel de navegación, seleccione Reglas.

   b. Elija el nombre de una regla que utilice la condición de restricción de tamaño que desea eliminar.

   c. En el panel de la derecha, seleccione la condición de restricción de tamaño que desea eliminar de la regla y, a continuación, elija Remove selected condition (Eliminar condición seleccionada).

   d. Repita los pasos b y c para todas las demás reglas que utilizan la condición de restricción de tamaño que desea eliminar.

   e. En el panel de navegación, elija Size constraint (Restricción de tamaño).

   f. En el panel Size constraint conditions (Condiciones de restricción de tamaño), elija la condición de restricción de tamaño que desea eliminar.
6. Elija Delete (Eliminar) para eliminar la condición seleccionada.

Trabajar con condiciones de coincidencia de inyección de código SQL

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Los atacantes a veces insertan código SQL malicioso en solicitudes web con el objetivo de extraer datos de su base de datos. Para permitir o bloquear solicitudes web que parecen contener código SQL malicioso, cree una o varias condiciones de coincidencia de inyección de código SQL. Una condición de coincidencia de inyección de SQL identifica la parte de las solicitudes web, como la ruta del URI o la cadena de consulta, que desea que AWS WAF Classic inspeccione. Más adelante, cuando cree una ACL web, puede especificar si desea permitir o bloquear las solicitudes que parecen contener código SQL maliciosos.

Temas

Crear condiciones de coincidencia de inyecciones de código SQL

Al crear condiciones de coincidencia en las inyecciones de SQL, se especifican filtros que indican la parte de las solicitudes web que desea que AWS WAF Classic inspeccione para detectar código SQL malintencionado, como el URI o la cadena de consulta. Puede añadir más de un filtro a una condición de coincidencia de inyección de código SQL o puede crear una condición independiente para cada filtro. Así es como cada configuración afecta al comportamiento de AWS WAF Classic:

- Más de un filtro por condición de coincidencia de inyección de SQL (recomendado): cuando se agrega una condición de coincidencia de inyección de SQL que contiene varios filtros a una regla y se agrega la regla a una ACL web, una solicitud web solo necesita coincidir con uno de los

filtros de la condición de coincidencia de inyección de SQL para que AWS WAF Classic permita o bloquee la solicitud en función de esa condición.

Por ejemplo, suponga que crea una condición de coincidencia de inyección de código SQL y que dicha condición contiene dos filtros. Un filtro indica a AWS WAF Classic que inspeccione el URI en busca de código SQL malintencionado y el otro indica a AWS WAF Classic que inspeccione la cadena de consulta. AWS WAF Classic permite o bloquea las solicitudes si parecen contener código SQL malintencionado en el URI o en la cadena de consulta.

- Un filtro por condición de coincidencia de inyección de SQL: al añadir las condiciones de coincidencia de inyección de SQL independientes a una regla y añadir la regla a una ACL web, las solicitudes web deben cumplir todas las condiciones para que AWS WAF Classic permita o bloquee las solicitudes en función de esas condiciones.

  Supongamos que crea dos condiciones y que cada condición contiene uno de los dos filtros del ejemplo anterior. Al añadir ambas condiciones a la misma regla y añadir la regla a una ACL web, AWS WAF Classic solo permite o bloquea las solicitudes cuando tanto el URI como la cadena de consulta parecen contener código SQL malintencionado.

> **Note**
>
> Al añadir una condición de coincidencia de inyección de SQL a una regla, también puede configurar la AWS WAF versión clásica para que permita o bloquee las solicitudes web que no parezcan contener código SQL malintencionado.

Para crear una condición de coincidencia de inyección de código SQL

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, seleccione SQL injection (Inyección de código SQL).
3. Elija Create condition.
4. Especifique la configuración de filtro aplicable. Para obtener más información, consulte Valores que se especifican al crear o editar condiciones de coincidencia de inyecciones de código SQL.
5. Elija Add another filter.

6. Si desea añadir otro filtro, repita los pasos 4 y 5.
7. Cuando haya terminado de añadir filtros, seleccione Create.

Valores que se especifican al crear o editar condiciones de coincidencia de inyecciones de código SQL

Al crear o actualizar una condición de coincidencia de inyección de código SQL, debe especificar los siguientes valores:

Nombre

Es el nombre de la condición de coincidencia de inyección de código SQL.

El nombre solo puede contener caracteres alfanuméricos (A-Z, a-z, 0-9) o los siguientes caracteres especiales: _-!"#`+*},./. No se puede cambiar el nombre de una condición después de crearla.

Parte de la solicitud para filtrar en

Elige la parte de cada solicitud web que quieres que AWS WAF Classic inspeccione para detectar código SQL malintencionado:

Encabezado

Un encabezado de solicitud específico, por ejemplo, el encabezado `User-Agent` o `Referer`. Si elige Header, indique el nombre del encabezado en el campo Header.

Método HTTP

El método HTTP indica el tipo de operación que la solicitud pide al origen que lleve a cabo. CloudFront admite los siguientes métodos: `DELETEGET`,`HEAD`, `OPTIONSPATCH`,`POST`, y`PUT`.

Cadena de consulta

Es la parte de una URL que aparece después de un carácter `?`, si hay alguno.

> **Note**
>
> En situaciones de coincidencia de inyecciones de código SQL, recomendamos elegir All query parameters (values only) (Todos los parámetros de consulta [solo valores]) en vez de Query string (Cadena de consulta) para Part of the request to filter on (Parte de la solicitud que se va a filtrar).

URI

La ruta del URI de la solicitud, que identifica el recurso, por ejemplo, `/images/daily-ad.jpg`. Esto no incluye la cadena de consulta ni los componentes del fragmento del URI. Para obtener información, consulte Identificador uniforme de recursos (URI): sintaxis genérica.

A menos que se especifique una transformación, el URI no se normaliza y se inspecciona tal y como lo AWS recibe del cliente como parte de la solicitud. Una transformación reformateará el URI según se especifique.

Cuerpo

Es la parte de una solicitud que contiene los datos adicionales que desea enviar a su servidor web como cuerpo de la solicitud HTTP, por ejemplo, los datos de un formulario.

> **Note**
>
> Si, por el contrario, elige Cuerpo para el valor de Parte de la consulta que se va a filtrar, AWS WAF Classic solo inspeccionará los primeros 8192 bytes (8 KB). Para permitir o bloquear solicitudes cuyo cuerpo tenga más de 8192 bytes, puede crear una condición de restricción de tamaño. (AWS WAF Classic obtiene la longitud del cuerpo de los encabezados de las solicitudes). Para obtener más información, consulte Trabajar con condiciones de restricción de tamaño.

Parámetro de consulta único (solo valor)

Cualquier parámetro que haya definido como parte de la cadena de consulta. Por ejemplo, si la URL es «www.xyz.com? UserName =abc& SalesRegion =seattle», puede añadir un filtro al parámetro o. UserNameSalesRegion

Si elige Single query parameter (value only) (Parámetro de consulta único [solo valor]), también debe especificar un Query parameter name (Nombre de parámetro de consulta). Este es el parámetro de la cadena de consulta que va a inspeccionar, como o. UserNameSalesRegion La longitud máxima del Query parameter name (Nombre de parámetro de consulta) es de 30 caracteres. Query parameter name (Nombre de parámetro de consulta) no distingue entre mayúsculas y minúsculas. Por ejemplo, si lo especificas UserNamecomo nombre del parámetro de consulta, coincidirá con todas las variantes UserName, como username y userName.

Todos los parámetros de consulta (solo valores)

Al igual que con el parámetro de consulta único (solo valor), pero en lugar de inspeccionar el valor de un solo parámetro, AWS WAF Classic inspecciona el valor de todos los parámetros de la cadena de consulta para detectar posibles códigos SQL malintencionados. Por ejemplo, si la dirección URL es «www.xyz.com? UserName =abc& SalesRegion =seattle» y selecciona Todos los parámetros de la consulta (solo valores), AWS WAF Classic activará una coincidencia si el valor de alguno de ellos contiene un posible código SQL malicioso. UserNameSalesRegion

Encabezado

Si selecciona Encabezado como parte de la solicitud por la que desea filtrar, elija un encabezado de la lista de encabezados más comunes o introduzca el nombre del encabezado que desee AWS WAF que Classic inspeccione para detectar códigos SQL malintencionados.

Transformación

Una transformación reformatea una solicitud web antes de que AWS WAF Classic la inspeccione. De este modo, se eliminan algunos de los formatos poco habituales que los atacantes utilizan en las solicitudes web para evitar AWS WAF la versión clásica.

Solo puede especificar un único tipo de transformación de texto.

Las transformaciones pueden realizar las siguientes operaciones:

Ninguna

AWS WAF Classic no realiza ninguna transformación de texto en la solicitud web antes de inspeccionarla para comprobar si coincide con la cadena de Value.

Cambiar a minúsculas

AWS WAF Classic convierte las letras mayúsculas (A-Z) en minúsculas (a-z).

Descodificar en HTML

AWS WAF La versión clásica reemplaza los caracteres codificados en HTML por caracteres no codificados:

- Sustituye `"` por &
- Sustituye ` ` por un espacio de no separación
- Sustituye `<` por <

- Sustituye `>` por >
- Sustituye los caracteres representados con formato hexadecimal, `&#xhhhh;`, por los caracteres correspondientes
- Sustituye los caracteres representados con formato decimal, `&#nnnn;`, por los caracteres correspondientes

Normalizar espacios en blanco

AWS WAF La versión clásica reemplaza los siguientes caracteres por un carácter de espacio (32 decimales):

- \f, salto de página, 12 decimales
- \t, pestaña, 9 decimales
- \n, línea nueva, 10 decimales
- \r, salto de línea, 13 decimales
- \v, pestaña vertical, 11 decimales
- espacio de no separación, 160 decimales

Además, esta opción sustituye varios espacios por un espacio.

Simplificar la línea de comandos

Para las solicitudes que contienen los comandos de línea de comandos del sistema operativo, utilice esta opción para realizar las siguientes transformaciones:

- Eliminar los siguientes caracteres: \ " ' ^
- Eliminar los espacios delante de los siguientes caracteres: / (
- Sustituir los siguientes caracteres por un espacio: , ;
- Sustituir varios espacios por un espacio
- Convertir las mayúsculas (A-Z) en minúsculas (a-z)

Descodificar la URL

Descodifique una solicitud de URL codificada.

Agregar y eliminar filtros en una condición de coincidencia de inyecciones de código SQL

Puede añadir o eliminar filtros en una condición de coincidencia de inyección de código SQL. Para cambiar un filtro, añada uno nuevo y elimine el viejo.

Para añadir o eliminar filtros en una condición de coincidencia de inyección de código SQL

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, seleccione SQL injection (Inyección de código SQL).
3. Elija la condición para la que desea añadir o eliminar filtros.
4. Para añadir filtros, siga los siguientes pasos:

   a. Elija Add filter (Agregar filtro).

   b. Especifique la configuración de filtro aplicable. Para obtener más información, consulte Valores que se especifican al crear o editar condiciones de coincidencia de inyecciones de código SQL.

   c. Elija Add (Agregar).
5. Para eliminar filtros, siga los siguientes pasos:

   a. Seleccione el filtro que desea eliminar.

   b. Elija Delete filter (Eliminar filtro).

Eliminar condiciones de coincidencia de inyecciones de código SQL

Si desea eliminar una condición de coincidencia de inyección de código SQL, primero debe eliminar todos los filtros de la condición y borrar la condición de todas las reglas que la utilizan, tal y como se describe en el siguiente procedimiento.

Para eliminar una condición de coincidencia de inyección de código SQL

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, seleccione SQL injection (Inyección de código SQL).
3. En el panel Condiciones de coincidencia de inyección de código SQL, elija la condición de inyección de código SQL que desea eliminar.
4. En el panel de la derecha, elija la pestaña Associated rules (Reglas asociadas).

Si la lista de reglas que utilizan la condición de coincidencia de inyección de código SQL está vacía, vaya al paso 6. Si la lista contiene alguna regla, anótela y continúe con el paso 5.

5. Para eliminar la condición de coincidencia de inyección de código SQL de las reglas que la utilizan, siga los siguientes pasos:

   a. En el panel de navegación, seleccione Reglas.

   b. Elija el nombre de una regla que utilice la condición de coincidencia de inyección de código SQL que desea eliminar.

   c. En el panel de la derecha, seleccione la condición de coincidencia de inyección de código SQL que desea eliminar de la regla y elija Remove selected condition (Eliminar condición seleccionada).

   d. Repita los pasos b y c para todas las demás reglas que utilizan la condición de coincidencia de inyección de código SQL que desea eliminar.

   e. En el panel de navegación, seleccione SQL injection (Inyección de código SQL).

   f. En el panel Condiciones de coincidencia de inyección de código SQL, elija la condición de inyección de código SQL que desea eliminar.

6. Elija Delete (Eliminar) para eliminar la condición seleccionada.

Trabajar con condiciones de coincidencia de cadena

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Si desea permitir o bloquear las solicitudes web en función de las cadenas que aparecen en las solicitudes, cree una o más condiciones de coincidencia de cadena. Una condición de coincidencia de cadenas identifica la cadena que desea buscar y la parte de las solicitudes web, como un encabezado específico o la cadena de consulta, que desea que AWS WAF Classic inspeccione en busca de la cadena. Más adelante, cuando cree una ACL web, puede especificar si desea permitir o bloquear las solicitudes que contienen la cadena.

Temas

Crear una condición de coincidencia de cadena

Al crear condiciones de coincidencia de cadenas, se especifican filtros que identifican la cadena que se quiere buscar y la parte de las solicitudes web que se desea que AWS WAF Classic inspeccione en busca de esa cadena, como el URI o la cadena de consulta. Puede añadir más de un filtro a una condición de coincidencia de cadena o bien puede crear una condición de coincidencia de cadena independiente para cada filtro. Así es como cada configuración afecta al comportamiento de la AWS WAF versión clásica:

- Condición de coincidencia de un filtro por cadena: al añadir las condiciones de coincidencia de cadenas independientes a una regla y añadir la regla a una ACL web, las solicitudes web deben cumplir todas las condiciones para que AWS WAF Classic permita o bloquee las solicitudes en función de esas condiciones.

  Por ejemplo, suponga que crea dos condiciones. Una coincide con las solicitudes web que contienen el valor `BadBot` en el encabezado `User-Agent`. La otra coincide con las solicitudes web que contienen el valor `BadParameter` en cadenas de consulta. Al añadir ambas condiciones a la misma regla y añadir la regla a una ACL web, la AWS WAF versión clásica solo permite o bloquea las solicitudes cuando contienen ambos valores.
- Más de un filtro por condición de coincidencia de cadenas: cuando se agrega una condición de coincidencia de cadenas que contiene varios filtros a una regla y se agrega la regla a una ACL web, una solicitud web solo necesita coincidir con uno de los filtros de la condición de coincidencia de cadenas para que la AWS WAF versión clásica permita o bloquee la solicitud en función de una condición.

  Supongamos que crea una condición en lugar de dos y que la única condición contiene los mismos dos filtros que en el ejemplo anterior. AWS WAF Classic permite o bloquea las solicitudes si están contenidas `BadBot` en el `User-Agent` encabezado o `BadParameter` en la cadena de consulta.

> **Note**
>
> Al añadir una condición de coincidencia de cadenas a una regla, también puede configurar la AWS WAF versión clásica para permitir o bloquear las solicitudes web que no coincidan con los valores de la condición.

Para crear una condición de coincidencia de cadena

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, elija String and regex matching (Coincidencia de cadenas y regex).
3. Elija Create condition.
4. Especifique la configuración de filtro aplicable. Para obtener más información, consulte Valores que se pueden especificar al crear o editar condiciones de coincidencia de cadena.
5. Elija Add filter (Agregar filtro).
6. Si desea añadir otro filtro, repita los pasos 4 y 5.
7. Cuando haya terminado de añadir filtros, seleccione Create.

Valores que se pueden especificar al crear o editar condiciones de coincidencia de cadena

Al crear o actualizar una condición de coincidencia de cadena, debe especificar los siguientes valores:

Nombre

Escriba un nombre para la condición de coincidencia de cadena. El nombre solo puede contener caracteres alfanuméricos (A-Z, a-z, 0-9) o los siguientes caracteres especiales: _-!"#`+*},./. No se puede cambiar el nombre de una condición después de crearla.

Tipo

Elija Coincidencia de cadena.

Parte de la solicitud para filtrar en

Elija la parte de cada solicitud web que desee que AWS WAF Classic inspeccione para ver si coincide con la cadena que especificó en Value:

Encabezado

Un encabezado de solicitud específico, por ejemplo, el encabezado `User-Agent` o `Referer`. Si elige Header, indique el nombre del encabezado en el campo Header.

Método HTTP

El método HTTP indica el tipo de operación que la solicitud pide al origen que lleve a cabo. CloudFront admite los siguientes métodos: `DELETE`, `GET`, `HEAD`, `OPTIONS`, `PATCH`, `POST`, y `PUT`.

Cadena de consulta

Es la parte de una URL que aparece después de un carácter `?`, si hay alguno.

URI

La ruta del URI de la solicitud, que identifica el recurso, por ejemplo, `/images/daily-ad.jpg`. Esto no incluye la cadena de consulta ni los componentes del fragmento del URI. Para obtener información, consulte Identificador uniforme de recursos (URI): sintaxis genérica.

A menos que se especifique una transformación, el URI no se normaliza y se inspecciona tal y como lo AWS recibe del cliente como parte de la solicitud. Una transformación reformateará el URI según se especifique.

Cuerpo

Es la parte de una solicitud que contiene los datos adicionales que desea enviar a su servidor web como cuerpo de la solicitud HTTP, por ejemplo, los datos de un formulario.

> **Note**
>
> Si, por el contrario, elige Cuerpo para el valor de Parte de la consulta que se va a filtrar, AWS WAF Classic solo inspeccionará los primeros 8192 bytes (8 KB). Para permitir o bloquear solicitudes cuyo cuerpo tenga más de 8192 bytes, puede crear una condición de restricción de tamaño. (AWS WAF Classic obtiene la longitud del cuerpo de los encabezados de las solicitudes). Para obtener más información, consulte Trabajar con condiciones de restricción de tamaño.

Parámetro de consulta único (solo valor)

Cualquier parámetro que haya definido como parte de la cadena de consulta. Por ejemplo, si la URL es «www.xyz.com? UserName =abc& SalesRegion =seattle», puede añadir un filtro al parámetro o. UserNameSalesRegion

Si hay parámetros duplicados en la cadena de consulta, los valores se evalúan como "OR". Es decir, ambos valores activarán una coincidencia. Por ejemplo, en la URL «www.xyz.com? SalesRegion =boston& SalesRegion =seattle», si aparece «boston» o «seattle» en Value to match, se activará una coincidencia.

Si elige Single query parameter (value only) (Parámetro de consulta único [solo valor]), también debe especificar un Query parameter name (Nombre de parámetro de consulta). Este es el parámetro de la cadena de consulta que va a inspeccionar, como o. UserNameSalesRegion La longitud máxima del Query parameter name (Nombre de parámetro de consulta) es de 30 caracteres. Query parameter name (Nombre de parámetro de consulta) no distingue entre mayúsculas y minúsculas. Por ejemplo, si lo especificas UserNamecomo nombre del parámetro de consulta, coincidirá con todas las variantes UserName, como username y userName.

Todos los parámetros de consulta (solo valores)

Similar al parámetro de consulta único (solo valor), pero en lugar de inspeccionar el valor de un solo parámetro, AWS WAF Classic inspecciona el valor de todos los parámetros de la cadena de consulta para ver si el valor coincide. Por ejemplo, si la URL es «www.xyz.com? UserName =abc& SalesRegion =seattle» y selecciona Todos los parámetros de la consulta (solo valores), AWS WAF Classic activará una coincidencia si el valor de alguno UserNamede ellos se especifica como el valor que debe coincidir. SalesRegion

Encabezado (solo cuando "Parte de la solicitud para filtrar en" es "Encabezado")

Si seleccionó Encabezado de la parte de la lista de solicitudes que desea filtrar, elija un encabezado de la lista de encabezados comunes o introduzca el nombre del encabezado que desee que Classic inspeccione. AWS WAF

Tipo de coincidencia

En la parte de la solicitud que desee que inspeccione AWS WAF Classic, elija dónde debe aparecer la cadena Value con la que desea que coincida con este filtro:

Contiene

La cadena aparece en cualquier lugar de la parte especificada de la solicitud.

Contiene palabra

La parte especificada de la solicitud web debe incluir Value to match (Valor que debe coincidir) y Value to match debe contener únicamente caracteres alfanuméricos o guion bajo (A-Z, a-z, 0-9 o _). Además, Value to match debe ser una palabra, lo que significa una de las siguientes opciones:

- Value to match (Valor que debe coincidir) coincide exactamente con el valor de la parte especificada de la solicitud web, como, por ejemplo, el valor de un encabezado.
- Value to match (Valor que debe coincidir) está al principio de la parte especificada de la solicitud web y le sigue un carácter que no es alfanumérico ni guion bajo (_), por ejemplo, `BadBot;`.
- Value to match (Valor que debe coincidir) está al final de la parte especificada de la solicitud web y le precede un carácter que no es alfanumérico ni guion bajo (_), por ejemplo, `;BadBot`.
- Value to match (Valor que debe coincidir) está en la mitad de la parte especificada de la solicitud web y va precedida y seguida de caracteres que no son alfanuméricos ni guion bajo (_), por ejemplo, `-BadBot;`.

Coincidencia exacta

La cadena y el valor de la parte especificada de la solicitud son idénticas.

Empieza por

La cadena aparece al principio de la parte especificada de la solicitud.

Acaba con

La cadena aparece al final de la parte especificada de la solicitud.

Transformación

Una transformación reformatea una solicitud web antes de que AWS WAF Classic la inspeccione. Esto elimina algunos de los formatos poco habituales que los atacantes utilizan en las solicitudes web para evitar AWS WAF la versión clásica.

Solo puede especificar un único tipo de transformación de texto.

Las transformaciones pueden realizar las siguientes operaciones:

Ninguna

AWS WAF Classic no realiza ninguna transformación de texto en la solicitud web antes de inspeccionarla para comprobar si coincide con la cadena de Value.

Cambiar a minúsculas

AWS WAF Classic convierte las letras mayúsculas (A-Z) en minúsculas (a-z).

Descodificar en HTML

AWS WAF La versión clásica reemplaza los caracteres codificados en HTML por caracteres no codificados:

- Sustituye `"` por &
- Sustituye ` ` por un espacio de no separación
- Sustituye `<` por <
- Sustituye `>` por >
- Sustituye los caracteres representados con formato hexadecimal, `&#xhhhh;`, por los caracteres correspondientes
- Sustituye los caracteres representados con formato decimal, `&#nnnn;`, por los caracteres correspondientes

Normalizar espacios en blanco

AWS WAF La versión clásica reemplaza los siguientes caracteres por un carácter de espacio (32 decimales):

- \f, salto de página, 12 decimales
- \t, pestaña, 9 decimales
- \n, línea nueva, 10 decimales
- \r, salto de línea, 13 decimales
- \v, pestaña vertical, 11 decimales
- espacio de no separación, 160 decimales

Además, esta opción sustituye varios espacios por un espacio.

Simplificar la línea de comandos

Si le preocupa que un atacante inyecte un comando de la línea de comandos del sistema operativo y utilice un formato inusual para ocultar parte o todo el comando, utilice esta opción para realizar las siguientes transformaciones:

- Eliminar los siguientes caracteres: \ " ' ^
- Eliminar los espacios delante de los siguientes caracteres: / (
- Sustituir los siguientes caracteres por un espacio: , ;
- Sustituir varios espacios por un espacio
- Convertir las mayúsculas (A-Z) en minúsculas (a-z)

Descodificar la URL

Descodifique una solicitud de URL codificada.

El valor se codifica con base64

Si el valor de Value to match (Valor que debe coincidir) tiene codificación base64, seleccione esta casilla de verificación. Utilice la codificación base64 para especificar caracteres no imprimibles, como pestañas y saltos de línea, que los atacantes incluyen en sus solicitudes.

Valor que debe coincidir

Especifique el valor que desea que AWS WAF Classic busque en las solicitudes web. La longitud máxima es de 50 bytes. Si su valor tiene codificación base64, la longitud máxima de 50 bytes se aplica al valor antes de codificarlo.

Agregar y eliminar filtros en una condición de coincidencia de cadena

Puede añadir o eliminar filtros en una condición de coincidencia de cadena. Para cambiar un filtro, añada uno nuevo y elimine el viejo.

Para añadir o eliminar filtros en una condición de coincidencia de cadena

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, elija String and regex matching (Coincidencia de cadenas y regex).
3. Elija la condición para la que desea añadir o eliminar filtros.
4. Para añadir filtros, siga los siguientes pasos:

   a. Elija Add filter (Agregar filtro).
   b. Especifique la configuración de filtro aplicable. Para obtener más información, consulte Valores que se pueden especificar al crear o editar condiciones de coincidencia de cadena.

c. Elija Add (Agregar).

5. Para eliminar filtros, siga los siguientes pasos:

   a. Seleccione el filtro que desea eliminar.

   b. Elija Eliminar filtro.

Eliminar condiciones de coincidencia de cadena

Si desea eliminar una condición de coincidencia de cadena, primero debe eliminar todos los filtros de la condición y borrar la condición de todas las reglas que la utilizan, tal y como se describe en el siguiente procedimiento.

Para eliminar una condición de coincidencia de cadena

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.

2. Quite la condición de coincidencia de cadena de las reglas que la utilizan:

   a. En el panel de navegación, seleccione Reglas.

   b. Elija el nombre de una regla que utilice la condición de coincidencia de cadena que desea eliminar.

   c. En el panel de la derecha, elija Edit rule (Editar regla).

   d. Elija la X situada al lado de la condición que desea eliminar.

   e. Seleccione Actualizar.

   f. Repita estos pasos para todas las demás reglas que utilizan la condición de coincidencia de cadena que desea eliminar.

3. Quite los filtros de la condición que desea eliminar:

   a. En el panel de navegación, elija String and regex matching (Coincidencia de cadenas y regex).

   b. Elija el nombre de la condición de coincidencia de cadena que desea eliminar.

   c. En el panel de la derecha, elija la casilla de verificación situada junto a Filter para seleccionar todos los filtros.

   d. Elija Delete filter (Eliminar filtro).

4. En el panel de navegación, elija String and regex matching (Coincidencia de cadenas y regex).
5. En el panel String and regex match conditions, elija la condición de coincidencia de cadena que desea eliminar.
6. Elija Delete (Eliminar) para eliminar la condición seleccionada.

Trabajar con condiciones de coincidencia de regex

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Si desea permitir o bloquear las solicitudes web en función de las cadenas que coinciden con un patrón de expresión regular (regex) que aparece en las solicitudes, cree una o más condiciones de coincidencia de regex. Una condición de coincidencia de expresiones regulares es un tipo de condición de coincidencia de cadenas que identifica el patrón que desea buscar y la parte de las solicitudes web, como un encabezado específico o la cadena de consulta, que desea que AWS WAF Classic inspeccione para detectar el patrón. Más adelante, cuando cree una ACL web, puede especificar si desea permitir o bloquear las solicitudes que contienen el patrón.

Temas

- Crear una condición de coincidencia de regex
- Los valores que especifique al crear o editar las condiciones de RegEx coincidencia
- Editar una condición de coincidencia de regex

Crear una condición de coincidencia de regex

Al crear condiciones de coincidencia de regex, debe especificar conjuntos de patrones que identifican la cadena (con una expresión regular) que desea buscar. A continuación, añada esos conjuntos de patrones a los filtros que especifican la parte de las solicitudes web que desea que AWS WAF Classic inspeccione en busca de ese conjunto de patrones, como el URI o la cadena de consulta.

Puede añadir varias expresiones regulares a un único conjunto de patrones. Si lo hace, esas expresiones se combinan con un OR. Es decir, una solicitud web coincidirá con el conjunto de patrones si la parte correspondiente de la solicitud coincide con cualquiera de las expresiones que se enumeran.

Al añadir una condición de coincidencia de expresiones regulares a una regla, también puede configurar AWS WAF Classic para permitir o bloquear las solicitudes web que no coincidan con los valores de la condición.

AWS WAF Classic es compatible con la mayoría de las expresiones regulares compatibles con Perl (PCRE) estándar. Sin embargo, no se admiten las siguientes:

- Referencias a elementos anteriores y subexpresiones de captura
- Aserciones arbitrarias de ancho cero
- Referencias de subrutinas y patrones recursivos
- Patrones condicionales
- Verbos de control de búsqueda de datos anteriores
- La directiva \C de byte único
- La directiva \R de coincidencia de nueva línea
- El inicio \K de la directiva de restablecimiento de coincidencia
- Llamadas y código incrustado
- Cuantificadores atómicos de agrupamiento y posesivos

Para crear una condición de coincidencia de regex

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, elija String and regex matching (Coincidencia de cadenas y regex).
3. Elija Create condition.
4. Especifique la configuración de filtro aplicable. Para obtener más información, consulte Los valores que especifique al crear o editar las condiciones de RegEx coincidencia.

5. Elija Create pattern set and add filter (Crear conjunto de patrones y agregar filtro) (si ha creado un nuevo conjunto de patrones) o Add filter (Add filter) si ha utilizado un conjunto de patrones existente.
6. Seleccione Crear.

Los valores que especifique al crear o editar las condiciones de RegEx coincidencia

Al crear o actualizar una condición de coincidencia de regex, debe especificar los siguientes valores:

Nombre

Escriba un nombre para la condición de coincidencia de regex. El nombre solo puede contener caracteres alfanuméricos (A-Z, a-z, 0-9) o los siguientes caracteres especiales: _-!"#`+*},./. No se puede cambiar el nombre de una condición después de crearla.

Tipo

Elija Regex match.

Parte de la solicitud para filtrar en

Elija la parte de cada solicitud web que desee que AWS WAF Classic inspeccione para ver si coincide con el patrón que especificó en Value:

Encabezado

Un encabezado de solicitud específico, por ejemplo, el encabezado `User-Agent` o `Referer`. Si elige Header, indique el nombre del encabezado en el campo Header.

Método HTTP

El método HTTP indica el tipo de operación que la solicitud pide al origen que lleve a cabo. CloudFront admite los siguientes métodos: `DELETEGET`,`HEAD`, `OPTIONSPATCH`,`POST`, y`PUT`.

Cadena de consulta

Es la parte de una URL que aparece después de un carácter `?`, si hay alguno.

URI

La ruta del URI de la solicitud, que identifica el recurso, por ejemplo, `/images/daily-ad.jpg`. Esto no incluye la cadena de consulta ni los componentes del fragmento del URI. Para obtener información, consulte Identificador uniforme de recursos (URI): sintaxis genérica.

A menos que se especifique una transformación, el URI no se normaliza y se inspecciona tal y como lo AWS recibe del cliente como parte de la solicitud. Una transformación reformateará el URI según se especifique.

Cuerpo

Es la parte de una solicitud que contiene los datos adicionales que desea enviar a su servidor web como cuerpo de la solicitud HTTP, por ejemplo, los datos de un formulario.

> **Note**
>
> Si, por el contrario, elige Cuerpo para el valor de Parte de la consulta que se va a filtrar, AWS WAF Classic solo inspeccionará los primeros 8192 bytes (8 KB). Para permitir o bloquear solicitudes cuyo cuerpo tenga más de 8192 bytes, puede crear una condición de restricción de tamaño. (AWS WAF Classic obtiene la longitud del cuerpo de los encabezados de las solicitudes). Para obtener más información, consulte Trabajar con condiciones de restricción de tamaño.

Parámetro de consulta único (solo valor)

Cualquier parámetro que haya definido como parte de la cadena de consulta. Por ejemplo, si la URL es «www.xyz.com? UserName =abc& SalesRegion =seattle», puede añadir un filtro al parámetro o. UserNameSalesRegion

Si hay parámetros duplicados en la cadena de consulta, los valores se evalúan como "OR". Es decir, ambos valores activarán una coincidencia. Por ejemplo, en la URL «www.xyz.com? SalesRegion =boston& SalesRegion =seattle», un patrón que coincida con «boston» o «seattle» en Value to match activará una coincidencia.

Si elige Single query parameter (value only) (Parámetro de consulta único [solo valor]), también debe especificar un Query parameter name (Nombre de parámetro de consulta). Este es el parámetro de la cadena de consulta que inspeccionará, como o. UserNameSalesRegion La longitud máxima del Query parameter name (Nombre de parámetro de consulta) es de 30 caracteres. Query parameter name (Nombre de parámetro de consulta) no distingue entre mayúsculas y minúsculas. Por ejemplo, si lo especificas UserNamecomo nombre del parámetro de consulta, coincidirá con todas las variantes UserName, como username y userName.

Todos los parámetros de consulta (solo valores)

Similar al parámetro de consulta único (solo valor), pero en lugar de inspeccionar el valor de un solo parámetro, AWS WAF Classic inspecciona el valor de todos los parámetros de la cadena de consulta para comprobar si coincide con el patrón especificado en el valor. Por ejemplo, en la URL «www.xyz.com? UserName =abc& SalesRegion =seattle», un patrón de Value to match que coincida con el valor de o provoque una coincidencia. UserNameSalesRegion

Encabezado (solo cuando "Parte de la solicitud para filtrar en" es "Encabezado")

Si seleccionó Encabezado de la parte de la solicitud que desea filtrar en la lista, elija un encabezado de la lista de encabezados comunes o introduzca el nombre del encabezado que desee que Classic inspeccione. AWS WAF

Transformación

Una transformación reformatea una solicitud web antes de que AWS WAF Classic la inspeccione. De este modo, se eliminan algunos de los formatos poco habituales que los atacantes utilizan en las solicitudes web para evitar AWS WAF la versión clásica.

Solo puede especificar un único tipo de transformación de texto.

Las transformaciones pueden realizar las siguientes operaciones:

Ninguna

AWS WAF Classic no realiza ninguna transformación de texto en la solicitud web antes de inspeccionarla para comprobar si coincide con la cadena de Value.

Cambiar a minúsculas

AWS WAF Classic convierte las letras mayúsculas (A-Z) en minúsculas (a-z).

Descodificar en HTML

AWS WAF La versión clásica reemplaza los caracteres codificados en HTML por caracteres no codificados:

- Sustituye `"` por &
- Sustituye ` ` por un espacio de no separación
- Sustituye `<` por <
- Sustituye `>` por >

- Sustituye los caracteres representados con formato hexadecimal, `&#xhhhh;`, por los caracteres correspondientes
- Sustituye los caracteres representados con formato decimal, `&#nnnn;`, por los caracteres correspondientes

Normalizar espacios en blanco

AWS WAF La versión clásica reemplaza los siguientes caracteres por un carácter de espacio (32 decimales):

- \f, salto de página, 12 decimales
- \t, pestaña, 9 decimales
- \n, línea nueva, 10 decimales
- \r, salto de línea, 13 decimales
- \v, pestaña vertical, 11 decimales
- espacio de no separación, 160 decimales

Además, esta opción sustituye varios espacios por un espacio.

Simplificar la línea de comandos

Si le preocupa que un atacante inyecte un comando de la línea de comandos del sistema operativo y utilice un formato inusual para ocultar parte o todo el comando, utilice esta opción para realizar las siguientes transformaciones:

- Eliminar los siguientes caracteres: \ " ' ^
- Eliminar los espacios delante de los siguientes caracteres: / (
- Sustituir los siguientes caracteres por un espacio: , ;
- Sustituir varios espacios por un espacio
- Convertir las mayúsculas (A-Z) en minúsculas (a-z)

Descodificar la URL

Descodifique una solicitud de URL codificada.

Patrón de expresión regular que coincide con la solicitud

Puede elegir un conjunto de patrones existente o crear uno nuevo. Si crea uno nuevo, especifique lo siguiente:

Nombre del nuevo patrón

Introduzca un nombre y, a continuación, especifique el patrón de expresiones regulares que desea que busque AWS WAF Classic.

Si añade varias expresiones regulares a un conjunto de patrones, esas expresiones se combinan con un OR. Es decir, una solicitud web coincidirá con el conjunto de patrones si la parte correspondiente de la solicitud coincide con cualquiera de las expresiones que se enumeran.

La longitud máxima de Value to match (Valor que debe coincidir) es 70 caracteres.

Editar una condición de coincidencia de regex

Puede realizar los siguientes cambios en una condición de coincidencia de regex existente:

- Eliminar un patrón de un conjunto de patrones existentes
- Añadir un patrón a un conjunto de patrones existentes
- Eliminar un filtro para una condición de coincidencia de regex existente
- Agregue un filtro a una condición de coincidencia de regex existente (solo puede tener un filtro en una condición de coincidencia de expresiones regulares; por tanto, para agregar un filtro, debe eliminar primero el filtro existente).
- Eliminar una condición de coincidencia de regex existente

> **Note**
>
> No puede añadir ni eliminar un conjunto de patrones de un filtro existente. Debe editar el conjunto de patrones, o eliminar el filtro y crear un nuevo filtro con un nuevo conjunto de patrones.

Para eliminar un patrón de un conjunto de patrones existentes

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.

2. En el panel de navegación, elija String and regex matching (Coincidencia de cadenas y regex).
3. Elija View regex pattern sets.
4. Elija el nombre del conjunto de patrones que desea editar.
5. Elija Editar.
6. Elija la X situada al lado del patrón que desea eliminar.
7. Seleccione Save (Guardar).

Para añadir un patrón a un conjunto de patrones existentes

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, elija String and regex matching (Coincidencia de cadenas y regex).
3. Elija View regex pattern sets.
4. Elija el nombre del conjunto de patrones que desea editar.
5. Elija Edit (Editar).
6. Escriba un nuevo patrón regex.
7. Elija el signo + situado junto al nuevo patrón.
8. Seleccione Guardar.

Para eliminar un filtro de una condición de coincidencia de regex existente

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, elija String and regex matching (Coincidencia de cadenas y regex).
3. Elija el nombre de la condición que tiene el filtro que desea eliminar.
4. Elija la casilla situada junto al filtro que desea eliminar.
5. Elija Delete filter (Eliminar filtro).

Para eliminar una condición de coincidencia de regex

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. Elimine el filtro de la condición regex. Consulte Para eliminar un filtro de una condición de coincidencia de regex existente para obtener instrucciones al respecto).
3. Quite la condición de coincidencia de regex de las reglas que la utilizan:
   a. En el panel de navegación, seleccione Reglas.
   b. Elija el nombre de una regla que utilice la condición de coincidencia de regex que desea eliminar.
   c. En el panel de la derecha, elija Edit rule (Editar regla).
   d. Elija la X situada al lado de la condición que desea eliminar.
   e. Seleccione Actualizar.
   f. Repita estos pasos para todas las demás reglas que utilizan la condición de coincidencia de regex que desea eliminar.
4. En el panel de navegación, elija String and regex matching (Coincidencia de cadenas y regex).
5. Seleccione el botón situado al lado de la condición que desea eliminar.
6. Elija Eliminar.

Para añadir o cambiar un filtro para una condición de coincidencia de regex existente

Solo puede haber un filtro en una condición de coincidencia de regex. Si desea añadir o cambiar el filtro, debe eliminar primero el filtro existente.

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. Elimine el filtro de la condición regex que desea cambiar. Consulte Para eliminar un filtro de una condición de coincidencia de regex existente para obtener instrucciones al respecto).
3. En el panel de navegación, elija String and regex matching (Coincidencia de cadenas y regex).
4. Elija el nombre de la condición que desea cambiar.

5. Elija Add filter (Agregar filtro).
6. Introduzca los valores adecuados para el nuevo filtro y elija Add (Agregar).

Trabajar con reglas

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Las reglas le permiten segmentar con precisión las solicitudes web que desea que AWS WAF Classic permita o bloquee especificando las condiciones exactas a las que debe prestar atención AWS WAF Classic. Por ejemplo, AWS WAF Classic puede comprobar las direcciones IP de las que se originan las solicitudes, las cadenas que contienen y dónde aparecen, y si las solicitudes parecen contener código SQL malintencionado.

Temas

- Crear una regla y agregar condiciones
- Agregar y eliminar condiciones en una regla
- Eliminar una regla
- AWS Marketplace grupos de reglas

Crear una regla y agregar condiciones

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Si añades más de una condición a una regla, la solicitud web debe cumplir todas las condiciones para que AWS WAF Classic permita o bloquee las solicitudes basadas en esa regla.

Para crear una regla y añadir condiciones

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, seleccione Reglas.
3. Seleccione Crear regla.
4. Escriba los siguientes valores:

   Nombre

   Escriba un nombre.

   CloudWatch nombre de la métrica

   Introduzca un nombre para la CloudWatch métrica que AWS WAF Classic creará y asociará a la regla. El nombre solo puede contener caracteres alfanuméricos (A-Z, a-z, 0-9), con una longitud máxima de 128 y una longitud mínima de 1. No puede contener espacios en blanco ni nombres de métricas reservados para la AWS WAF versión clásica, como «All» y «Default_Action».

   Tipo de regla

   Elija `Regular rule` o `Rate-based rule`. Las reglas basadas en tasas son idénticas a las reglas convencionales, pero también tienen en cuenta el número de solicitudes que proceden de una dirección IP en un período de cinco minutos. Para obtener más información sobre estos tipos de regla, consulte Cómo funciona AWS WAF Classic.

   Límite de frecuencia

   Para una regla basada en frecuencia, introduzca el número máximo de solicitudes que desea permitir en cualquier periodo de cinco minutos desde una dirección IP que coincida con las condiciones de la regla. El límite de frecuencia debe ser de 100 como mínimo.

   Puede especificar un límite de frecuencia solo o un límite de frecuencia y condiciones. Si especificas solo un límite de velocidad, AWS WAF coloca el límite en todas las direcciones

IP. Si especificas un límite de velocidad y condiciones, AWS WAF establece el límite en las direcciones IP que cumplan las condiciones.

Cuando una dirección IP alcanza el umbral del límite de velocidad, AWS WAF aplica la acción asignada (bloquear o contar) lo más rápido posible, normalmente en 30 segundos. Una vez realizada la acción, si transcurren cinco minutos sin ninguna solicitud de la dirección IP, se AWS WAF restablece el contador a cero.

5. Para añadir una condición a la regla, especifique los siguientes valores:

Cuando una solicitud incluye/excluye

Si desea que AWS WAF Classic permita o bloquee las solicitudes en función de los filtros de una condición, elija sí. Por ejemplo, si una condición de coincidencia de IP incluye el rango de direcciones IP 192.0.2.0/24 y desea que AWS WAF Classic permita o bloquee las solicitudes que provienen de esas direcciones IP, elija sí.

Si desea que AWS WAF Classic permita o bloquee las solicitudes en función de la inversa de los filtros de una condición, elija no hacerlo. Por ejemplo, si una condición de coincidencia de IP incluye el rango de direcciones IP 192.0.2.0/24 y desea que AWS WAF Classic permita o bloquee las solicitudes que no provengan de esas direcciones IP, elija no hacerlo.

coincide/se origina en

Elija el tipo de condición que desea añadir a la regla:

- Condiciones de coincidencia de scripting entre sitios: elija hacer coincidir al menos uno de los filtros en la condición de coincidencia de scripts entre sitios
- Condiciones de coincidencia de IP: elija originar desde una dirección IP en
- Condiciones de coincidencia geográfica: elija originar desde una ubicación geográfica en
- Condiciones de restricción de tamaño: elija coincidir con al menos uno de los filtros en la condición de restricción de tamaño
- Condiciones de coincidencia de inyección de código SQL: elija coincidir con al menos uno de los filtros en la condición de coincidencia de inyección de código SQL
- Condiciones de coincidencia de cadena: elija coincidir al menos uno de los filtros en la condición de coincidencia de cadena
- Condiciones de coincidencia de expresión regular: elija coincidir con al menos uno de los filtros en la condición de coincidencia de expresiones regulares

nombre de condición

Elija la condición que desea añadir a la regla. La lista muestra únicamente las condiciones del tipo que eligió en el paso anterior.

6. Para agregar otra condición a la regla, elija Agregar otra condición y repita los pasos 4 y 5. Tenga en cuenta lo siguiente:

   - Si agregas más de una condición, una solicitud web debe coincidir con al menos un filtro en cada condición para que AWS WAF Classic permita o bloquee las solicitudes en función de esa regla
   - Si agregas dos condiciones de coincidencia de IP a la misma regla, AWS WAF Classic solo permitirá o bloqueará las solicitudes que se originen en las direcciones IP que aparezcan en ambas condiciones de coincidencia de IP

7. Cuando haya terminado de añadir condiciones, seleccione Create.

Agregar y eliminar condiciones en una regla

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Puede cambiar una regla añadiendo o eliminando condiciones.

Para añadir o eliminar condiciones en una regla

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.

2. En el panel de navegación, seleccione Reglas.
3. Elija el nombre de la regla en la que desea añadir o quitar condiciones.
4. Seleccione Add rule (Agregar regla).

5. Para agregar una condición, elija Add condition (Agregar condición) y especifique los siguientes valores:

   Cuando una solicitud incluye/excluye

   Si desea que AWS WAF Classic permita o bloquee las solicitudes en función de los filtros de una condición, por ejemplo, las solicitudes web que se originan en el rango de direcciones IP 192.0.2.0/24, elija sí.

   Si desea que AWS WAF Classic permita o bloquee las solicitudes en función de la inversa de los filtros de una condición, elija no hacerlo. Por ejemplo, si una condición de coincidencia de IP incluye el rango de direcciones IP 192.0.2.0/24 y desea que AWS WAF Classic permita o bloquee las solicitudes que no provengan de esas direcciones IP, elija no hacerlo.

   coincide/se origina en

   Elija el tipo de condición que desea añadir a la regla:

   - Condiciones de coincidencia de scripting entre sitios: elija hacer coincidir al menos uno de los filtros en la condición de coincidencia de scripts entre sitios
   - Condiciones de coincidencia de IP: elija originar desde una dirección IP en
   - Condiciones de coincidencia geográfica: elija originar desde una ubicación geográfica en
   - Condiciones de restricción de tamaño: elija coincidir con al menos uno de los filtros en la condición de restricción de tamaño
   - Condiciones de coincidencia de inyección de código SQL: elija coincidir con al menos uno de los filtros en la condición de coincidencia de inyección de código SQL
   - Condiciones de coincidencia de cadena: elija coincidir al menos uno de los filtros en la condición de coincidencia de cadena
   - Condiciones de coincidencia de expresión regular: elija coincidir con al menos uno de los filtros en la condición de coincidencia de expresiones regulares

   nombre de condición

   Elija la condición que desea añadir a la regla. La lista muestra únicamente las condiciones del tipo que eligió en el paso anterior.

6. Para quitar una condición, seleccione la X que hay a la derecha del nombre de la condición
7. Seleccione Actualizar.

Eliminar una regla

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Si desea eliminar una regla, primero debe borrar la regla de la ACL web que la utiliza y, a continuación, las condiciones que incluye la regla.

Para eliminar una regla

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. Para eliminar la regla de las ACL web que la utilizan, siga los pasos siguientes para cada ACL web:

   a. En el panel de navegación, seleccione Web ACLs (ACL web).

   b. Elija el nombre de una ACL web que utiliza la regla que desea borrar.

   c. Elija la pestaña Rules.

   d. Elija Edit web ACL (Editar ACL web).

   e. Elija la X que hay a la derecha de la regla que desea eliminar y, a continuación, elija Actualizar.
3. En el panel de navegación, seleccione Reglas.
4. Seleccione el nombre de la regla que desea eliminar.
5. Elija Delete (Eliminar).

AWS Marketplace grupos de reglas

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la versión más reciente. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

AWS WAF La versión clásica proporciona grupos de AWS Marketplace reglas para ayudarle a proteger sus recursos. AWS Marketplace Los grupos de reglas son conjuntos de ready-to-use reglas predefinidas redactadas y actualizadas por AWS empresas AWS asociadas.

Algunos grupos de AWS Marketplace reglas están diseñados para ayudar a proteger tipos específicos de aplicaciones web WordPress, como Joomla o PHP. Otros grupos de AWS Marketplace reglas ofrecen una amplia protección contra las amenazas conocidas o las vulnerabilidades más comunes de las aplicaciones web, como las que figuran en la lista de los 10 principales de OWASP.

Puede instalar un único grupo de AWS Marketplace reglas de su AWS socio preferido y también puede añadir sus propias reglas AWS WAF clásicas personalizadas para aumentar la protección. Si está sujeto a la conformidad normativa de PCI o HIPAA, podría utilizar grupos de reglas de AWS Marketplace para cumplir los requisitos de firewall de las aplicaciones web.

AWS Marketplace Los grupos de reglas están disponibles sin contratos a largo plazo ni compromisos mínimos. Si se suscribe a un grupo de reglas, se le cobrará una cuota mensual (prorrateada por hora) y cuotas continuas de solicitudes en función del volumen. Para obtener más información, consulta los precios AWS WAF clásicos y la descripción de cada grupo de AWS Marketplace reglas en AWS Marketplace.

Actualizaciones automáticas

Mantenerse al día sobre el panorama de amenazas en constante cambio puede llevar mucho tiempo y resultar caro. AWS Marketplace Los grupos de reglas pueden ahorrarle tiempo a la hora de implementar y utilizar la AWS WAF versión clásica. Otra ventaja es que AWS nuestros AWS socios actualizan automáticamente los grupos de AWS Marketplace reglas cuando surgen nuevas vulnerabilidades y amenazas.

Muchos de nuestros socios reciben una notificación de nuevas vulnerabilidades antes de su revelación pública. Pueden actualizar sus grupos de reglas e implementarlos en su cuenta antes de que una nueva amenaza sea de dominio público. Muchos de ellos también disponen de equipos de investigación de amenazas que estudian y analizan las últimas amenazas para crear las reglas más pertinentes.

Acceso a las reglas de un grupo de AWS Marketplace reglas

Cada grupo de AWS Marketplace reglas proporciona una descripción completa de los tipos de ataques y vulnerabilidades contra los que está diseñado para protegerse. Para proteger la propiedad intelectual de los proveedores de grupos de reglas, no puede ver las reglas individuales que hay dentro de un grupo de reglas. Esta restricción también ayuda a impedir que usuarios malintencionados diseñen amenazas que eludan específicamente las reglas publicadas.

Como no puede ver las reglas individuales de un AWS Marketplace grupo de reglas, tampoco puede editar ninguna AWS Marketplace regla de un grupo de reglas. Sin embargo, puede excluir reglas específicas de un grupo de reglas. Esto es lo que se conoce como "excepción de grupo de reglas". La exclusión de reglas no elimina esas reglas. En su lugar, cambia la acción de las reglas a `COUNT`. Por lo tanto, las solicitudes que coinciden con una regla excluida se recuentan pero no se bloquean. Recibirá métricas COUNT para cada regla excluida.

La exclusión de reglas puede resultar útil a la hora de solucionar problemas de grupos de reglas que bloquean el tráfico de forma inesperada (falsos positivos). Una técnica de resolución de problemas consiste en identificar la regla específica del grupo de reglas que está bloqueando el tráfico deseado y, a continuación, deshabilitar (excluir) esa regla específica.

Además de excluir reglas específicas, para refinar su protección, puede habilitar o deshabilitar grupos de reglas enteros, así como elegir la acción del grupo de reglas que desea realizar. Para obtener más información, consulte Uso de grupos de AWS Marketplace reglas.

Cuotas

Solo puede habilitar un grupo de AWS Marketplace reglas. También puede habilitar un grupo de reglas personalizado que cree mediante AWS Firewall Manager. Estos grupos de reglas cuentan para la cuota máxima de 10 reglas por ACL web. Por lo tanto, puede tener un grupo de AWS Marketplace reglas, un grupo de reglas personalizado y hasta ocho reglas personalizadas en una única ACL web.

Precios

Para conocer los precios por grupos de AWS Marketplace reglas, consulte los precios AWS WAF clásicos y la descripción de cada grupo de AWS Marketplace reglas AWS Marketplace.

Uso de grupos de AWS Marketplace reglas

Puede suscribirse y cancelar su suscripción a los grupos de AWS Marketplace reglas en la consola AWS WAF clásica. También puede excluir reglas específicas de un grupo de reglas.

Uso y suscripción a un grupo de reglas de AWS Marketplace

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, seleccione Marketplace.
3. En la sección Available marketplace products, elija el nombre de un grupo de reglas para ver los detalles y la información sobre precios.
4. Si desea suscribirse al grupo de reglas, elija Continue.

   > **Note**
   >
   > Si no desea suscribirse a este grupo de reglas, solo tiene que cerrar esta página en su navegador.

5. Elija Set up your account.
6. Añada el grupo de reglas a una ACL web, como si se tratase de una regla individual. Para obtener más información, consulte Creación de una ACL web o Edición de una ACL web.

   > **Note**
   >
   > Al añadir un grupo de reglas a una ACL web, la acción que define para el grupo de reglas (No override (No anular) u Override to count [Anular para recuento]) se denomina acción de anulación del grupo de reglas. Para obtener más información, consulte Invalidar un grupo de reglas.

Cancelación de la suscripción a un grupo de reglas de AWS Marketplace

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. Quite el grupo de reglas de todas las ACL web. Para obtener más información, consulte Edición de una ACL web.
3. En el panel de navegación, seleccione Marketplace.
4. Elija Manage your subscriptions.
5. Elija Cancel subscription situada junto al nombre del grupo de reglas cuya suscripción desea cancelar.
6. Elija Yes, cancel subscription.

Para excluir una regla de un grupo de reglas (excepción de grupo de reglas)

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. Si aún no está activado, habilite el registro AWS WAF clásico. Para obtener más información, consulte Registro de información del tráfico de la ACL web. Utilice los registros AWS WAF clásicos para identificar los ID de las reglas que desee excluir. Suelen ser reglas que bloquean solicitudes legítimas.
3. En el panel de navegación, seleccione Web ACLs (ACL web).
4. Elegir el nombre de la ACL web que desea editar. Esto abre una página con los detalles de la ACL web en el panel derecho.

   > **Note**
   >
   > El grupo de reglas que desea editar debe estar asociado a una ACL web antes de poder excluir una regla de ese grupo de reglas.
5. En la pestaña Reglas en el panel de la derecha, elija Editar ACL web.
6. En la sección Rule group exceptions (Excepciones de grupo de reglas), expanda el grupo de reglas que desea editar.

7. Elija la X situada junto a la regla que desea excluir. Puede identificar el ID de regla correcto mediante los registros AWS WAF clásicos.
8. Seleccione Actualizar.

   La exclusión de reglas no elimina esas reglas del grupo de reglas. En su lugar, cambia la acción de las reglas a `COUNT`. Por lo tanto, las solicitudes que coinciden con una regla excluida se recuentan pero no se bloquean. Recibirá métricas `COUNT` para cada regla excluida.

   > **Note**
   >
   > Puede utilizar este mismo procedimiento para excluir reglas de grupos de reglas personalizadas que ha creado en AWS Firewall Manager. Sin embargo, en lugar de excluir una regla de un grupo de reglas personalizadas con estos pasos, también puede editar simplemente un grupo de reglas personalizado con los pasos que se describen en Añadir y eliminar reglas de un grupo de reglas AWS WAF clásico.

Invalidar un grupo de reglas

AWS Marketplace Los grupos de reglas tienen dos acciones posibles: no anular y anular para contabilizar. Si desea probar el grupo de reglas, establezca la acción en Override to count. Esta acción del grupo de reglas anula cualquier acción de bloqueo especificada por las reglas individuales incluidas en el grupo. Es decir, si la acción del grupo de reglas está establecida en Override to count, en lugar de bloquear potencialmente las solicitudes coincidentes en función de la acción de las reglas individuales incluidas en el grupo, dichas solicitudes se contabilizarán. Por el contrario, si establece la acción del grupo de reglas en No override, se utilizarán las acciones de las reglas individuales incluidas en el grupo.

Solucionar problemas de grupos de reglas de AWS Marketplace

Si descubre que un grupo de AWS Marketplace reglas bloquea el tráfico legítimo, lleve a cabo los siguientes pasos.

Para solucionar problemas de un grupo de reglas de AWS Marketplace

1. Excluya las reglas específicas que están bloqueando el tráfico legítimo. Puede identificar qué reglas bloquean qué solicitudes mediante los registros AWS WAF clásicos. Para obtener más información acerca de cómo excluir reglas, consulte Para excluir una regla de un grupo de reglas (excepción de grupo de reglas).

2. Si excluir reglas específicas no resuelve el problema, puede cambiar la acción del grupo de AWS Marketplace reglas de No anular a anular el recuento. Esto permite el paso de la solicitud web, independientemente de las acciones de las reglas individuales incluidas en el grupo de reglas. Esto también te proporciona CloudWatch las métricas de Amazon para el grupo de reglas.
3. Tras configurar la acción del grupo de AWS Marketplace reglas como Anular el recuento, ponte en contacto con el equipo de atención al cliente del proveedor del grupo de reglas para seguir solucionando el problema. Para obtener información de contacto, consulte la lista de grupos de reglas en las páginas de listas de productos en AWS Marketplace.

Contactar con el servicio de atención al cliente

Si tienes problemas con la AWS WAF versión clásica o con un grupo de reglas gestionado por él AWS, ponte en contacto con nosotros. AWS Support Si tiene problemas con un grupo de reglas gestionado por un AWS socio, póngase en contacto con el equipo de atención al cliente de ese socio. Para encontrar la información de contacto del socio, consulte la lista del socio en AWS Marketplace.

Creación y venta de grupos de reglas de AWS Marketplace

Si quiere vender grupos de AWS Marketplace reglas AWS Marketplace, consulte Cómo vender su software en AWS Marketplace.

Trabajar con ACL web

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Al agregar reglas a una ACL web, debe especificar si desea que AWS WAF Classic permita o bloquee las solicitudes en función de las condiciones de las reglas. Si agrega más de una regla a una ACL web, AWS WAF Classic evalúa cada solicitud según las reglas en el orden en que se enumeran en la ACL web. Cuando una solicitud web cumple todas las condiciones de una regla,

AWS WAF Classic realiza inmediatamente la acción correspondiente (permitir o bloquear) y no evalúa la solicitud en función del resto de las reglas de la ACL web, si las hubiera.

Si una solicitud web no cumple ninguna de las reglas de una ACL web, AWS WAF Classic lleva a cabo la acción predeterminada que especificó para la ACL web. Para obtener más información, consulte Decidir sobre la acción predeterminada para una ACL web.

Si desea probar una regla antes de empezar a utilizarla para permitir o bloquear las solicitudes, puede configurar AWS WAF Classic para que cuente las solicitudes web que cumplen las condiciones de la regla. Para obtener más información, consulte Probar ACL web.

Temas

Decidir sobre la acción predeterminada para una ACL web

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Al crear y configurar una ACL web, la primera y más importante decisión que debe tomar es si la acción predeterminada debe ser que la AWS WAF versión clásica permita las solicitudes web o las bloquee. La acción predeterminada indica lo que desea que haga AWS WAF Classic después de inspeccionar una solicitud web para detectar todas las condiciones que especifique, y la solicitud web no cumple ninguna de esas condiciones:

- Permitir: si desea permitir que la mayoría de los usuarios pueda obtener acceso a su sitio web, pero desea bloquear el acceso a atacantes cuyas solicitudes provienen de direcciones IP específicas o cuyas solicitudes parecen contener código SQL malicioso o valores específicos, elija Permitir como la acción predeterminada.
- Bloquear: si desea evitar que la mayoría de posibles usuarios obtenga acceso a su sitio web, pero desea permitir el acceso a los usuarios cuyas solicitudes provienen de direcciones IP específicas o cuyas solicitudes contienen valores específicos, elija Bloquear como la acción predeterminada.

Muchas decisiones que se toman después de haber escogido una acción predeterminada dependen de si se desea permitir o bloquear la mayoría de solicitudes web. Por ejemplo, si desea permitir la mayoría de las solicitudes, entonces las condiciones de coincidencia que cree en general deberían incluir las solicitudes web que desea bloquear, como las siguientes:

- Las solicitudes que provengan de direcciones IP que realizan un número excesivo de solicitudes
- Las solicitudes que proceden de países en los que no opera o que con frecuencia son origen de ataques
- Las solicitudes que incluyen valores falsos en el encabezado User-Agent
- Las solicitudes que parecen incluir código SQL malicioso

Creación de una ACL web

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Para crear una ACL web

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.

2. Si es la primera vez que usa la AWS WAF versión clásica, elija Ir a la AWS WAF versión clásica y, a continuación, Configurar Web ACL. Si ya ha utilizado la AWS WAF versión clásica, seleccione ACL web en el panel de navegación y, a continuación, elija Crear ACL web.
3. En Nombre de ACL web, escriba un nombre.

   > **Note**
   >
   > No se puede cambiar el nombre después de crear la ACL web.

4. Para el nombre de la CloudWatch métrica, cambie el nombre predeterminado, si procede. El nombre solo puede contener caracteres alfanuméricos (A-Z, a-z, 0-9), con una longitud máxima de 128 y una longitud mínima de 1. No puede contener espacios en blanco ni nombres de métricas reservados para la AWS WAF versión clásica, como «All» y «Default_Action».

   > **Note**
   >
   > No se puede cambiar el nombre después de crear la ACL web.

5. En Región, seleccione una región.
6. En AWS resource, seleccione el recurso que desea asociar a esta ACL web y, a continuación, elija Next.
7. Si ya has creado las condiciones que quieres que AWS WAF Classic utilice para inspeccionar tus solicitudes web, selecciona Siguiente y continúa con el paso siguiente.

   Si todavía no ha creado las condiciones, hágalo ahora. Para obtener más información, consulte los temas siguientes:

   - Trabajar con condiciones de coincidencia de scripting entre sitios
   - Trabajar con condiciones de coincidencia de IP
   - Trabajar con condiciones de coincidencia geográfica
   - Trabajar con condiciones de restricción de tamaño
   - Trabajar con condiciones de coincidencia de inyección de código SQL
   - Trabajar con condiciones de coincidencia de cadena
   - Trabajar con condiciones de coincidencia de regex
8. Si ya ha creado las reglas o los grupos de reglas (o se ha suscrito a un grupo de AWS Marketplace reglas) que desea añadir a esta ACL web, añada las reglas a la ACL web:

a. En la lista Rules, elija una regla.

b. Elija Add rule to web ACL (Añadir regla a ACL web).

c. Repita los pasos a y b hasta que haya añadido todas las reglas que desea añadir a esta ACL web.

d. Vaya al paso 10.

9. Si todavía no ha creado reglas, puede añadirlas ahora:

a. Elija Create rule (Crear regla).

b. Escriba los siguientes valores:

Nombre

Escriba un nombre.

CloudWatch nombre de la métrica

Introduzca un nombre para la CloudWatch métrica que AWS WAF Classic creará y asociará a la regla. El nombre solo puede contener caracteres alfanuméricos (A-Z, a-z, 0-9), con una longitud máxima de 128 y una longitud mínima de 1. No puede contener espacios en blanco ni se pueden utilizar nombres de métricas reservados para AWS WAF Classic, como "All" y "Default_Action".

> **Note**
>
> Después de crear la regla, no se puede cambiar el nombre de las métricas.

c. Para añadir una condición a la regla, especifique los siguientes valores:

Cuando una solicitud incluye/excluye

Si desea que AWS WAF Classic permita o bloquee las solicitudes en función de los filtros de una condición, por ejemplo, las solicitudes web que se originan en el rango de direcciones IP 192.0.2.0/24, elija sí.

Si desea que AWS WAF Classic permita o bloquee las solicitudes en función de la inversa de los filtros de una condición, elija no hacerlo. Por ejemplo, si una condición de coincidencia de IP incluye el rango de direcciones IP 192.0.2.0/24 y desea que AWS

WAF Classic permita o bloquee las solicitudes que no provengan de esas direcciones IP, elija no hacerlo.

coincide/se origina en

Elija el tipo de condición que desea añadir a la regla:

- Condiciones de coincidencia de scripting entre sitios: elija hacer coincidir al menos uno de los filtros en la condición de coincidencia de scripts entre sitios
- Condiciones de coincidencia de IP: elija originar desde una dirección IP en
- Condiciones de coincidencia geográfica: elija originar desde una ubicación geográfica en
- Condiciones de restricción de tamaño: elija coincidir con al menos uno de los filtros en la condición de restricción de tamaño
- Condiciones de coincidencia de inyección de código SQL: elija coincidir con al menos uno de los filtros en la condición de coincidencia de inyección de código SQL
- Condiciones de coincidencia de cadena: elija coincidir al menos uno de los filtros en la condición de coincidencia de cadena
- Condiciones de coincidencia de regex: elija coincidir con al menos uno de los filtros en la condición de coincidencia de expresiones regulares

nombre de condición

Elija la condición que desea añadir a la regla. La lista muestra únicamente las condiciones del tipo que eligió en la lista anterior.

d. Para agregar otra condición a la regla, elija Add another condition (Agregar otra condición) y, a continuación, repita los pasos b y c. Tenga en cuenta lo siguiente:

   - Si agregas más de una condición, una solicitud web debe coincidir con al menos un filtro en cada condición para que AWS WAF Classic permita o bloquee las solicitudes en función de esa regla.
   - Si agregas dos condiciones de coincidencia de IP a la misma regla, AWS WAF Classic solo permitirá o bloqueará las solicitudes que se originen en las direcciones IP que aparezcan en ambas condiciones de coincidencia de IP.

e. Repita el paso 9 hasta que haya creado todas las reglas que desea añadir a esta ACL web.

f. Seleccione Crear.

g. Continúe con el paso 10.

10. Para cada regla o grupo de reglas de la ACL web, elija el tipo de administración que desea que proporcione AWS WAF Classic, de la siguiente manera:

    - Para cada regla, elija si quiere que AWS WAF Classic permita, bloquee o cuente las solicitudes web en función de las condiciones de la regla:
      - Permitir: API Gateway CloudFront o Application Load Balancer responde con el objeto solicitado. En el caso de CloudFront que el objeto no esté en la memoria caché perimetral, CloudFront reenvía la solicitud al origen.
      - Bloquear: API Gateway CloudFront o Application Load Balancer responde a la solicitud con un código de estado HTTP 403 (Prohibido). CloudFront también puede responder con una página de error personalizada. Para obtener más información, consulte Uso de AWS WAF Classic con páginas de error CloudFront personalizadas.
      - Recuento: AWS WAF Classic incrementa un contador de solicitudes que cumplen las condiciones de la regla y, a continuación, continúa inspeccionando la solicitud web en función de las demás reglas de la ACL web.

        Para obtener más información acerca de cómo utilizar Count (Recuento) para probar una ACL web antes de comenzar a utilizarla para permitir o bloquear solicitudes web, consulte Recontar las solicitudes web que coinciden con las reglas en una ACL web.
    - Para cada grupo de reglas, establezca la acción de anulación para el grupo de reglas:
      - No anular: hace que se accionen las reglas individuales del grupo de reglas que se va a utilizar.
      - Anular para recuento: anula cualquier acción de bloqueo especificada por las reglas individuales del grupo, de modo que solo se hace el recuento de todas las solicitudes coincidentes.

    Para obtener más información, consulte Invalidar un grupo de reglas.
11. Si desea cambiar el orden de las reglas en la ACL web, utilice las flechas de la columna Orden. AWS WAF Classic inspecciona las solicitudes web en función del orden en que aparecen las reglas en la ACL web.
12. Si desea eliminar una regla que ha añadido a la ACL web, elija la x de la fila de la regla.
13. Elija la acción predeterminada para ACL web. Esta es la acción que realiza AWS WAF Classic cuando una solicitud web no cumple las condiciones de ninguna de las reglas de esta ACL web. Para obtener más información, consulte Decidir sobre la acción predeterminada para una ACL web.

14. Elija Review and create.
15. Revise la configuración de la ACL web y elija Confirm and create (Confirmar y crear).

Asociar o desasociar una ACL web con una API de Amazon API Gateway, una CloudFront distribución o un Application Load Balancer

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Para asociar o desasociar una ACL web, siga el procedimiento aplicable. Tenga en cuenta que también puede asociar una ACL web a una CloudFront distribución al crear o actualizar la distribución. Para obtener más información, consulta Cómo usar la AWS WAF versión clásica para controlar el acceso a tu contenido en la Guía para CloudFront desarrolladores de Amazon.

Las restricciones siguientes se aplican cuando se asocia una ACL web:

- Cada API, Application Load Balancer y CloudFront distribución de API Gateway se pueden asociar a una sola ACL web.
- Las ACL web asociadas a una CloudFront distribución no se pueden asociar a una API de Application Load Balancer o API Gateway. Sin embargo, la ACL web se puede asociar a otras CloudFront distribuciones.

Para asociar una ACL web a una API Gateway, API, CloudFront distribución o Application Load Balancer

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, seleccione Web ACLs (ACL web).

3. Elija el nombre de la ACL web que desee asociar a una API, CloudFront distribución o Application Load Balancer de API Gateway. Esto abre una página con los detalles de la ACL web en el panel derecho.
4. En la pestaña Reglas, en Recursos de AWS que usan esta ACL web, elija Agregar asociación.
5. Cuando se le solicite, utilice la lista de recursos para elegir la API, CloudFront distribución o Application Load Balancer de API Gateway con la que desee asociar esta ACL web. Si elige un equilibrador de carga de aplicación, también debe especificar una región.
6. Elija Añadir.
7. Para asociar esta ACL web a una API API Gateway adicional, una CloudFront distribución u otro Application Load Balancer, repita los pasos 4 a 6.

Para desasociar una ACL web de una API Gateway, API, CloudFront distribución o Application Load Balancer

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, seleccione Web ACLs (ACL web).
3. Elija el nombre de la ACL web que desee desasociar de una API, CloudFront distribución o Application Load Balancer de API Gateway. Esto abre una página con los detalles de la ACL web en el panel derecho.
4. En la pestaña Reglas, en AWS Recursos que utilizan esta ACL web, elija la x para cada API, CloudFront distribución o Application Load Balancer de API Gateway de la que desee desasociar esta ACL web.

Edición de una ACL web

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Para añadir o eliminar reglas de una ACL web o cambiar la acción predeterminada, siga el siguiente procedimiento.

Para editar una ACL web

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, seleccione Web ACLs (ACL web).
3. Elegir el nombre de la ACL web que desea editar. Esto abre una página con los detalles de la ACL web en el panel derecho.
4. En la pestaña Reglas en el panel de la derecha, elija Editar ACL web.
5. Para añadir reglas a la ACL web, siga los siguientes pasos:

   a. En la lista Rules, elija la regla que desea añadir.

   b. Elija Add rule to web ACL (Añadir regla a ACL web).

   c. Repita los pasos a y b hasta que haya añadido todas las reglas que desea.
6. Si desea cambiar el orden de las reglas en la ACL web, utilice las flechas de la columna Orden. AWS WAF Classic inspecciona las solicitudes web en función del orden en que aparecen las reglas en la ACL web.
7. Para eliminar una regla de la ACL web, elija la x a la derecha de la fila de dicha regla. Esto no elimina la regla de la AWS WAF versión clásica, solo la elimina de esta ACL web.
8. Para cambiar la acción para una regla o la acción predeterminada para la ACL web, seleccione la opción preferida.

   > **Note**
   >
   > Al configurar la acción para un grupo de reglas o un grupo de AWS Marketplace reglas (a diferencia de una sola regla), la acción que se establece para el grupo de reglas (no anular o anular para contar) se denomina acción de anulación. Para más información, consulte Invalidar un grupo de reglas
9. Elija Guardar cambios.

Eliminación de una ACL web

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Para eliminar una ACL web, debe eliminar las reglas incluidas en la ACL web y desasociar todas CloudFront las distribuciones y los balanceadores de carga de aplicaciones de la ACL web. Realice el siguiente procedimiento.

Para eliminar una ACL web

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, seleccione Web ACLs (ACL web).
3. Elija el nombre de la ACL web que desea eliminar. Esto abre una página con los detalles de la ACL web en el panel derecho.
4. En la pestaña Reglas en el panel de la derecha, elija Editar ACL web.
5. Para eliminar todas las reglas de la ACL web, elija la x a la derecha de la fila de cada regla. Esto no elimina las reglas de la AWS WAF versión clásica, solo las elimina de esta ACL web.
6. Seleccione Actualizar.
7. Desasocie la ACL web de todas las CloudFront distribuciones y balanceadores de carga de aplicaciones. En la pestaña Reglas, en AWS Recursos que utilizan esta ACL web, elija la x para cada API, CloudFront distribución o Application Load Balancer de API Gateway.
8. En la página ACL web, confirme que la ACL web que desea eliminar esté seleccionada y, a continuación, elija Delete (Eliminar).

Probar ACL web

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Para asegurarse de no configurar accidentalmente AWS WAF Classic para bloquear las solicitudes web que desee permitir o permitir las solicitudes que desee bloquear, le recomendamos que pruebe minuciosamente su ACL web antes de empezar a utilizarla en su sitio web o aplicación web.

Temas

- Recontar las solicitudes web que coinciden con las reglas en una ACL web
- Ver una muestra de las solicitudes web que API Gateway CloudFront o Application Load Balancer han reenviado a Classic AWS WAF

Recontar las solicitudes web que coinciden con las reglas en una ACL web

Al añadir reglas a una ACL web, debe especificar si quiere que AWS WAF Classic permita, bloquee o cuente las solicitudes web que cumplan todas las condiciones de esa regla. Recomendamos que empiece con la siguiente configuración:

- Configurar todas las reglas de una ACL web para contar solicitudes web
- Establecer la acción predeterminada para que la ACL web permita las solicitudes

En esta configuración, AWS WAF Classic inspecciona cada solicitud web en función de las condiciones de la primera regla. Si la solicitud web cumple todas las condiciones de esa regla, AWS WAF Classic incrementa un contador para esa regla. A continuación, AWS WAF Classic inspecciona la solicitud web en función de las condiciones de la siguiente regla. Si la solicitud cumple todas las condiciones de esa regla, AWS WAF Classic incrementa un contador para la regla. Esto continúa hasta que AWS WAF Classic haya inspeccionado la solicitud en función de las condiciones de todas tus reglas.

Una vez que haya configurado todas las reglas de una ACL web para contar las solicitudes y haya asociado la ACL web a una API, CloudFront distribución o Application Load Balancer de Amazon API Gateway, podrá ver los recuentos resultantes en un gráfico de Amazon CloudWatch. Para cada regla de una ACL web y para todas las solicitudes que API Gateway CloudFront o Application Load Balancer reenvíen a AWS WAF Classic para una ACL web, CloudWatch le permite:

- Ver los datos correspondientes a la hora anterior o a las tres horas anteriores
- Cambiar el intervalo entre puntos de datos
- Cambie el cálculo que se CloudWatch realiza con los datos, como el máximo, el mínimo, el promedio o la suma

> **Note**
>
> AWS WAF La versión clásica CloudFront es un servicio global y las métricas solo están disponibles si eliges la región EE. UU. Este (Virginia del Norte) en AWS Management Console. Si eliges otra región, no aparecerá ninguna métrica AWS WAF clásica en la CloudWatch consola.

Para ver los datos de las reglas de una ACL web

1. Inicia sesión AWS Management Console y abre la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación izquierdo, en Metrics, elija WAF.
3. Seleccione la casilla de verificación de la ACL web cuyos datos quiera ver.
4. Cambie la configuración aplicable:

   Estadística

   Elija el cálculo que se CloudWatch realizará con los datos.

   Intervalo de tiempo

   Elija si desea ver los datos correspondientes a la hora anterior o a las tres horas anteriores.

   Período

   Elija el intervalo entre puntos de datos del gráfico.

Reglas

Elija las reglas cuyos datos quiera ver.

Tenga en cuenta lo siguiente:

- Si acabas de asociar una ACL web a una API, CloudFront distribución o Application Load Balancer de API Gateway, es posible que tengas que esperar unos minutos para que los datos aparezcan en el gráfico y para que la métrica de la ACL web aparezca en la lista de métricas disponibles.
- Si asocias más de una API, CloudFront distribución o Application Load Balancer de API Gateway a una ACL web, los CloudWatch datos incluirán todas las solicitudes de todas las distribuciones asociadas a la ACL web.
- Puede colocar el cursor del ratón sobre un punto de datos para obtener más información.
- El gráfico no se actualiza por su cuenta de forma automática. Para actualizar la pantalla, elija el icono de actualización ().

5. (Opcional) Consulta información detallada sobre las solicitudes individuales que API Gateway CloudFront o Application Load Balancer han reenviado a AWS WAF Classic. Para obtener más información, consulte Ver una muestra de las solicitudes web que API Gateway CloudFront o Application Load Balancer han reenviado a Classic AWS WAF.
6. Si determina que una regla está interceptando solicitudes que no desea interceptar, cambie la configuración aplicable. Para obtener más información, consulte Crear y configurar una lista de control de acceso web (ACL web).

   Cuando crea que todas sus reglas interceptan solo las solicitudes correctas, cambie la acción de cada una de sus reglas a Allow o Block. Para obtener más información, consulte Edición de una ACL web.

Ver una muestra de las solicitudes web que API Gateway CloudFront o Application Load Balancer han reenviado a Classic AWS WAF

En la consola AWS WAF clásica, puedes ver una muestra de las solicitudes que API Gateway CloudFront o un Application Load Balancer han reenviado a AWS WAF Classic para su inspección. Para cada solicitud muestreada, puede ver datos detallados acerca de la solicitud, como la dirección

IP de origen y los encabezados incluidos en la solicitud. También puede ver con qué regla coincidió la solicitud y si la regla está configurada para permitir o bloquear solicitudes.

La muestra de solicitudes contiene hasta 100 solicitudes que coincidieron con todas las condiciones de cada regla y otras 100 solicitudes para la acción predeterminada, que se aplica a las solicitudes que no coincidieron con todas las condiciones de cada regla. Las solicitudes del ejemplo provienen de todas las API, ubicaciones CloudFront perimetrales o balanceadores de carga de aplicaciones de API Gateway que recibieron solicitudes de tu contenido en los últimos 15 minutos.

Para ver una muestra de las solicitudes web que API Gateway CloudFront o Application Load Balancer han reenviado a Classic AWS WAF

1. Inicie sesión en la AWS WAF consola AWS Management Console y ábrala en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.
2. En el panel de navegación, elija la ACL web cuyas solicitudes quiera ver.
3. En el panel de la derecha, elija la pestaña Requests.

   En la tabla Sampled requests se muestran los siguientes valores para cada solicitud:

   IP de origen

   La dirección IP desde la que se originó la solicitud o, si el espectador ha usado un proxy HTTP o un equilibrador de carga de aplicación para enviar la solicitud, la dirección IP del proxy o el equilibrador de carga de aplicación.

   URI

   La ruta del URI de la solicitud, que identifica el recurso, por ejemplo, `/images/daily-ad.jpg`. Esto no incluye la cadena de consulta ni los componentes del fragmento del URI. Para obtener información, consulte Identificador uniforme de recursos (URI): sintaxis genérica.

   Regla de coincidencias

   Identifica la primera regla de la ACL web para la que la solicitud web coincidió con todas las condiciones. Si una solicitud web no coincide con todas las condiciones de cada regla de la ACL web, el valor de Matches rule es Default.

Tenga en cuenta que cuando una solicitud web cumple todas las condiciones de una regla y la acción de esa regla es Contar, AWS WAF Classic continúa inspeccionando la solicitud web en función de las reglas posteriores de la ACL web. En este caso, una solicitud web podría aparecer dos veces en la lista de solicitudes muestreadas: una para la regla que tiene una acción de Count y otra vez para una regla posterior o para la acción predeterminada.

Acción

Indica si la acción de la regla correspondiente es Allow, Block o Count.

Time

La hora en que AWS WAF Classic recibió la solicitud de API Gateway CloudFront o de su Application Load Balancer.

4. Para mostrar información adicional sobre la solicitud, selecciona la flecha situada a la izquierda de la dirección IP de la solicitud. AWS WAF La versión clásica muestra la siguiente información:

IP de origen

La misma dirección IP como el valor de la columna Source IP de la tabla.

País

El código de país de dos letras del país desde el que se originó la solicitud. Si el espectador ha usado un proxy HTTP o un equilibrador de carga de aplicación para enviar la solicitud, este es el código de país de dos letras del país en el que se encuentra el proxy HTTP o un equilibrador de carga de aplicación.

Para obtener una lista de códigos de país de dos letras y los nombres de los países correspondientes, consulte la entrada de Wikipedia ISO 3166-1 alpha-2.

Método

El método de solicitud HTTP para la solicitud: `GET`, `HEAD`, `OPTIONS`, `PUT`, `POST`, `PATCH`, o bien `DELETE`.

URI

La misma URI que el valor de la columna URI de la tabla.

Encabezados de solicitudes

Los encabezados de la solicitud y los valores de encabezado de la solicitud.

5. Para actualizar la lista de solicitudes de muestra, elija Get new samples.

Trabajar con grupos de reglas AWS WAF clásicos para usarlos con AWS Firewall Manager

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la versión más reciente. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Un grupo de reglas AWS WAF clásico es un conjunto de reglas que se agregan a una AWS Firewall Manager política AWS WAF clásica. Puede crear su propio grupo de reglas o comprar un grupo de reglas administrado en él AWS Marketplace.

> **Important**
>
> Si desea agregar un grupo de AWS Marketplace reglas a su política de Firewall Manager, cada cuenta de su organización debe suscribirse primero a ese grupo de reglas. Una vez suscritas todas las cuentas, puede agregar el grupo de reglas a una política. Para obtener más información, consulte AWS Marketplace grupos de reglas.

Temas

- Creación de un grupo de reglas AWS WAF clásico
- Añadir y eliminar reglas de un grupo de reglas AWS WAF clásico

Creación de un grupo de reglas AWS WAF clásico

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los

ha migrado a la versión más reciente. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Al crear un grupo de reglas AWS WAF clásico para usarlo AWS Firewall Manager, se especifican las reglas que se van a añadir al grupo.

Para crear un grupo de reglas (consola)

1. Inicie sesión AWS Management Console con la cuenta de AWS Firewall Manager administrador que configuró en los requisitos previos y, a continuación, abra la consola del Firewall Manager enhttps://console.aws.amazon.com/wafv2/fms.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte Paso 2: Crear una cuenta de administrador AWS Firewall Manager predeterminada.

2. En el panel de navegación, elija Cambiar a la AWS WAF versión clásica.
3. En el panel de navegación AWS WAF clásico, elija Grupos de reglas.
4. Seleccione Create rule group (Crear grupo de reglas).

   > **Note**
   >
   > No se pueden añadir reglas basadas en frecuencia a un grupo de reglas.

5. Si ya ha creado las reglas que desea añadir al grupo de reglas, elija Use existing rules for this rule group (Usar reglas existentes para este grupo de reglas). Si desea crear nuevas reglas para añadirlas al grupo de reglas, elija Create rules and conditions for this rule group (Crear reglas y condiciones para este grupo de reglas).
6. Elija Siguiente.
7. Si decide crear reglas, siga los pasos para crearlas en Crear una regla y agregar condiciones.

> **Note**
>
> Utilice la consola AWS WAF clásica para crear sus reglas.

Cuando haya creado todas las reglas que necesite, vaya al siguiente paso.

8. Escriba un nombre de grupo de reglas.
9. Para añadir una regla al grupo de reglas, seleccione una regla y, a continuación, elija Add rule (Añadir regla). Elija si desea permitir, bloquear o contar solicitudes que coincidan con las condiciones de la regla. Para obtener más información acerca de las opciones, consulte Cómo funciona AWS WAF Classic.
10. Cuando haya terminado de añadir reglas, elija Create (Crear).

Puede probar su grupo de reglas agregándolo a una AWS WAF WebACL y configurando la acción WebACL en Override to Count. Esta acción anula cualquier acción que elija para las reglas incluidas en el grupo y solo cuenta las solicitudes coincidentes. Para obtener más información, consulte Creación de una ACL web.

Añadir y eliminar reglas de un grupo de reglas AWS WAF clásico

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la versión más reciente. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Puede añadir o eliminar reglas en un grupo de reglas AWS WAF clásico.

Si elimina una regla del grupo de reglas no elimina la propia regla. Solo elimina la regla del grupo de reglas.

Para añadir o eliminar reglas de un grupo de reglas (consola)

1. Inicie sesión AWS Management Console con la cuenta de AWS Firewall Manager administrador que configuró en los requisitos previos y, a continuación, abra la consola del Firewall Manager en https://console.aws.amazon.com/wafv2/fms.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte Paso 2: Crear una cuenta de administrador AWS Firewall Manager predeterminada.

2. En el panel de navegación, elija Cambiar a la AWS WAF versión clásica.
3. En el panel de navegación AWS WAF clásico, elija Grupos de reglas.
4. Elija el grupo de reglas que desea editar.
5. Elija Edit rule group (Editar grupo de reglas).
6. Para añadir reglas, siga estos pasos:

   a. Seleccione una regla y, a continuación, elija Add rule to rule group (Añadir regla a grupo de reglas). Elija si desea permitir, bloquear o contar solicitudes que coincidan con las condiciones de la regla. Para obtener más información acerca de las opciones, consulte Cómo funciona AWS WAF Classic. Repita el procedimiento para añadir más reglas al grupo de reglas.

      > **Note**
      >
      > No puede agregar reglas basadas en frecuencia al grupo de reglas.

   b. Seleccione Actualizar.
7. Para eliminar reglas, siga estos pasos:

   a. Elija la X situada al lado de la regla que desea eliminar. Repita el procedimiento para eliminar más reglas del grupo de reglas.

   b. Seleccione Actualizar.

Cómo empezar AWS Firewall Manager a activar las reglas AWS WAF clásicas

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Se puede utilizar AWS Firewall Manager para habilitar AWS WAF reglas, reglas AWS WAF clásicas, AWS Shield Advanced protecciones y grupos de seguridad de Amazon VPC. Los pasos de configuración difieren ligeramente en cada caso:

- Si desea utilizar el Firewall Manager para habilitar las reglas que utilizan la versión más reciente de AWS WAF, no utilice este tema. En su lugar, siga los pasos que se indican en Cómo empezar con AWS Firewall ManagerAWS WAF las políticas.
- Para usar el Firewall Manager para activar AWS Shield Advanced las protecciones, sigue los pasos que se indicanCómo empezar con AWS Firewall ManagerAWS Shield Advanced las políticas.
- Para usar Firewall Manager para habilitar los grupos de seguridad de Amazon VPC, siga los pasos que se indican en Introducción a las políticas de grupos de seguridad de AWS Firewall Manager Amazon VPC.

Para usar el Firewall Manager para habilitar las reglas AWS WAF clásicas, lleve a cabo los siguientes pasos en secuencia.

Temas

Paso 1: completar los requisitos previos

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Existen varios pasos obligatorios para preparar su cuenta de AWS Firewall Manager. Estos pasos se describen en AWS Firewall Manager requisitos previos. Complete todos los requisitos previos antes de continuar con Paso 2: Crear reglas.

Paso 2: Crear reglas

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

En este paso, se crean reglas mediante la AWS WAF versión clásica. Si ya tiene reglas AWS WAF clásicas con las que quiere usarlas AWS Firewall Manager, omita este paso y vaya aPaso 3: Crear un grupo de reglas.

> **Note**
>
> Usa la consola AWS WAF clásica para crear tus reglas.

Para crear reglas AWS WAF clásicas (consola)

- Cree sus reglas y, a continuación, añada sus condiciones a las reglas. Para obtener más información, consulte Crear una regla y agregar condiciones.

Ahora está preparado para ir a Paso 3: Crear un grupo de reglas.

Paso 3: Crear un grupo de reglas

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Un grupo de reglas es un conjunto de reglas que define qué acciones llevará a cabo si se cumplen un conjunto de condiciones específico. Puede usar grupos de reglas administrados desde AWS Marketplace y puede crear sus propios grupos de reglas. Para obtener información acerca de los grupos de reglas administrados, consulte AWS Marketplace grupos de reglas.

Para crear su propio grupo de reglas, siga el procedimiento que se indica a continuación.

Para crear un grupo de reglas (consola)

1. Inicie sesión AWS Management Console con la cuenta de AWS Firewall Manager administrador que configuró en los requisitos previos y, a continuación, abra la consola del Firewall Manager enhttps://console.aws.amazon.com/wafv2/fms.
2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Si no cumple los requisitos previos, la consola muestra instrucciones sobre cómo solucionar cualquier problema. Siga las instrucciones y, a continuación, comience de nuevo con este paso (crear un grupo de reglas). Si cumple los requisitos previos, elija Cerrar.
4. Elija Crear política.

   En Policy type (Tipo de política), seleccione AWS WAF Classic.
5. Seleccione Crear una AWS Firewall Manager política y agregue un nuevo grupo de reglas.

6. Elija una y Región de AWS, a continuación, elija Siguiente.
7. Dado que ya ha creado las reglas, no es necesario que cree condiciones. Elija Siguiente.
8. Dado que ya ha creado las reglas, ya no es necesario crearlas. Elija Siguiente.
9. Seleccione Create rule group (Crear grupo de reglas).
10. En Name (Nombre), escriba un nombre fácil de recordar.
11. Introduzca un nombre para la CloudWatch métrica que AWS WAF Classic creará y asociará al grupo de reglas. El nombre solo puede contener caracteres alfanuméricos (A-Z, a-z, 0-9) o los siguientes caracteres especiales: _-!"#`+*},./. No puede contener espacios en blanco.
12. Seleccione una regla y, a continuación, elija Add rule (Añadir regla). Una regla tiene una configuración de acción que le permite elegir si desea permitir, bloquear o contar solicitudes que coincidan con las condiciones de la regla. Para este tutorial, elija Count (Contar). Siga añadiendo reglas hasta que haya añadido todas las reglas que desea al grupo de reglas.
13. Seleccione Crear.

Ahora está preparado para ir a Paso 4: Crear y aplicar una política AWS Firewall ManagerAWS WAF clásica.

Paso 4: Crear y aplicar una política AWS Firewall ManagerAWS WAF clásica

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la versión más reciente. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Tras crear el grupo de reglas, se crea una AWS Firewall Manager AWS WAF política. Una AWS WAF política de Firewall Manager contiene el grupo de reglas que desea aplicar a sus recursos.

Para crear una AWS WAF política de Firewall Manager (consola)

1. Después de crear el grupo de reglas (el último paso del procedimiento anterior, Paso 3: Crear un grupo de reglas), la consola muestra la página Rule group summary (Resumen del grupo de reglas). Elija Siguiente.
2. En Name (Nombre), escriba un nombre fácil de recordar.
3. En Policy type (Tipo de política), elija WAF.
4. En Región, elija una Región de AWS. Para proteger CloudFront los recursos de Amazon, elige Global.

   Para proteger los recursos en varias regiones (distintas de CloudFront los recursos), debe crear políticas de Firewall Manager independientes para cada región.
5. Seleccione un grupo de reglas que desee añadir y, a continuación, elija Add rule group (Añadir grupo de reglas).
6. Una política dispone de dos posibles acciones: Action set by rule group (Acción establecida por el grupo de reglas) y Count (Contar). Si desea probar la política y el grupo de reglas, establezca la acción en Count (Contar). Esta acción anula cualquier acción de bloqueo especificada por el grupo de reglas incluido en la política. Es decir, si la acción de la política está establecida en Count (Contar), las solicitudes solo se contabilizan y no se bloquean. Por el contrario, si establece la acción de la política en Action set by rule group (Acción establecida por el grupo de reglas), se utilizan las acciones del grupo de reglas incluido en la política. Para este tutorial, elija Count (Contar).
7. Elija Siguiente.
8. Si desea incluir solo cuentas específicas en la política, o bien excluir de forma alternativa cuentas específicas de la política, seleccione Select accounts to include/exclude from this policy (optional) (Seleccionar cuentas que se van a incluir en/excluir de esta política (opcional)). Elija Include only these accounts in this policy (Incluir solo estas cuentas en esta política) o Exclude these accounts from this policy (Excluir estas cuentas de esta política). Solo puede elegir una opción. Elija Añadir. Seleccione los números de cuenta que se van a incluir o excluir y, a continuación, seleccione OK (Aceptar).

> **Note**
>
> Si no selecciona esta opción, Firewall Manager aplica una política a todas las cuentas de su organización en AWS Organizations. Si añade una nueva cuenta a la organización, Firewall Manager aplicará automáticamente la política a dicha cuenta.

9. Escoja los tipos de recursos que desea proteger.
10. Si solo desea proteger recursos con etiquetas específicas, o también si desea excluir recursos con etiquetas específicas, seleccione Use tags to include/exclude resources (Usar etiquetas para incluir/excluir recursos), introduzca las etiquetas y, a continuación, seleccione Include (Incluir) o Exclude (Excluir). Solo puede elegir una opción.

    Si escribe varias etiquetas (separadas por comas) y si un recurso tiene cualquiera de estas etiquetas, se considera una coincidencia.

    Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.
11. Seleccione Create and apply this policy to existing and new resources (Crear y aplicar esta política a los recursos nuevos y existentes).

    Esta opción crea una ACL web en cada cuenta aplicable de una organización y asocia la ACL web a los recursos especificados en las cuentas. AWS Organizations Esta opción también aplica la política a todos los nuevos recursos que coinciden con los criterios precedentes (tipo de recurso y etiquetas). Por otro lado, si elige Crear política pero no aplicarla a los recursos nuevos o existentes, Firewall Manager crea una ACL web en cada cuenta de la organización que cumplen los requisitos necesarios, pero no la aplica a ningún recurso. Deberá aplicar la política a los recursos posteriormente.
12. Deje la opción de Sustituir ACL web asociadas existentes con la configuración predeterminada.

    Cuando se selecciona esta opción, Firewall Manager eliminó todas las asociaciones ACL web existentes de los recursos dentro del ámbito antes de que se asocie las ACL web de la nueva política.
13. Elija Siguiente.
14. Revise la nueva política. Para realizar cualquier cambio, elija Edit (Editar). Cuando esté satisfecho con la política, elija Crear política.

Tutorial: Crear una política de AWS Firewall Manager con reglas jerárquicas

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Con AWS Firewall Manager, puede crear y aplicar políticas de protección AWS WAF clásicas que contengan reglas jerárquicas. Es decir, puede crear y aplicar determinadas reglas de forma centralizada, pero no delegar la creación y el mantenimiento de reglas específicas de la cuenta en otras personas. Puede monitorizar las reglas aplicadas de forma centralizada (comunes) para cualquier eliminación accidental o errónea, lo que garantiza que se apliquen de forma coherente. Las reglas específicas de la cuenta añaden protección aún más personalizada para las necesidades de los equipos individuales.

> **Note**
>
> En la última versión de AWS WAF, esta función viene integrada y no requiere ningún tratamiento especial. Si aún no utiliza la versión AWS WAF clásica, utilice la versión más reciente. Consulte Crear una AWS Firewall Manager política para AWS WAF.

En el siguiente tutorial se describe cómo crear un conjunto jerárquico de reglas de protección.

Temas

Paso 1: Designar una cuenta de administrador de Firewall Manager

Para AWS Firewall Manager utilizarla, debe designar una cuenta de su organización como cuenta de administrador del Firewall Manager. Esta cuenta puede ser la cuenta de administración o una cuenta miembro de la organización.

Puede utilizar la cuenta de administrador de Firewall Manager para crear un conjunto de reglas comunes que se aplican a otras cuentas de la organización. Otras cuentas de la organización no pueden cambiar estas reglas aplicadas de forma centralizada.

Para designar una cuenta como una cuenta de administrador de Firewall Manager y completar otros requisitos previos para utilizar Firewall Manager, consulte las instrucciones en AWS Firewall Manager requisitos previos. Si ya ha completado los requisitos previos, puede ir al paso 2 de este tutorial.

En este tutorial, haremos referencia a la cuenta de administrador como **`Firewall-Administrator-Account`**.

Paso 2: Crear un grupo de reglas mediante la cuenta de administrador de Firewall Manager

A continuación, cree un grupo de reglas a través de **`Firewall-Administrator-Account`**. Este grupo de reglas contiene las reglas comunes que aplicará a todas las cuentas de miembros que se rigen por la política que cree en el siguiente paso. Solo **`Firewall-Administrator-Account`** puede realizar cambios en estas reglas y en el grupo de reglas del contenedor.

En este tutorial, haremos referencia a este grupo de reglas del contenedor como **`Common-Rule-Group`**.

Para crear un grupo de reglas, consulte las instrucciones en Creación de un grupo de reglas AWS WAF clásico. Recuerde iniciar sesión en la consola mediante su cuenta de administrador de Firewall Manager (**`Firewall-Administrator-Account`**) al seguir estas instrucciones.

Paso 3: Crear una política de Firewall Manager y asociar el grupo de reglas comunes

Cree una política de Firewall Manager mediante **`Firewall-Administrator-Account`**. Cuando cree esta política, debe hacer lo siguiente:

- Añadir **`Common-Rule-Group`** a la nueva política.

- Incluir todas las cuentas de la organización a las que desee aplicar **`Common-Rule-Group`**.
- Añadir todos los recursos a los que desee aplicar **`Common-Rule-Group`**.

Para obtener instrucciones sobre cómo crear una política, consulte Creación de una AWS Firewall Manager política.

Esto crea una ACL web en cada cuenta especificada y añade **`Common-Rule-Group`** a cada una de esas ACL web. Después de crear la política, esta ACL web y las reglas comunes se implementan en todas las cuentas especificadas.

En este tutorial, haremos referencia a esta ACL web como **`Administrator-Created-ACL`**. Ya existe una **`Administrator-Created-ACL`** única en cada cuenta de miembro específica de la organización.

Paso 4: Agregar reglas específicas de la cuenta

Ahora cada cuenta de miembro de la organización puede añadir sus propias reglas específicas de la cuenta a la **`Administrator-Created-ACL`** que existe en su cuenta. Las reglas comunes que ya están en **`Administrator-Created-ACL`** vigor siguen aplicándose, junto con las nuevas reglas específicas de cada cuenta. AWS WAF inspecciona las solicitudes web en función del orden en que aparecen las reglas en la ACL web. Esto se aplica tanto a **`Administrator-Created-ACL`** como a las reglas específica de la cuenta.

Para añadir reglas a **`Administrator-Created-ACL`**, consulte Edición de una ACL web.

Conclusión

Ahora tiene una ACL web que contiene reglas comunes administradas por la cuenta de administrador de Firewall Manager, así como las reglas específicas de la cuenta mantenidas por cada cuenta de miembro.

La **`Administrator-Created-ACL`** de cada cuenta hace referencia al único **`Common-Rule-Group`**. Por lo tanto, los próximos cambios por la cuenta de administrador de Firewall Manager en **`Common-Rule-Group`** se aplicarán de forma inmediata en cada cuenta de miembro.

Las cuentas de miembros no pueden cambiar o eliminar las reglas comunes en **`Common-Rule-Group`**.

Las reglas específicas de la cuenta no afectan a otras cuentas.

Registro de información del tráfico de la ACL web

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

> **Note**
>
> No puede usar Amazon Security Lake para recopilar datos AWS WAF clásicos.

Puede habilitar el registro para obtener información detallada sobre el tráfico que analiza su ACL web. La información que se incluye en los registros incluye la hora en que AWS WAF Classic recibió la solicitud de su AWS recurso, la información detallada sobre la solicitud y la acción aplicada a la regla según la cual cada solicitud coincidió.

Para empezar, configure una instancia de Amazon Kinesis Data Firehose. Como parte de ese proceso, elija un destino para almacenar sus registros. A continuación, elija la ACL web para la que desea habilitar el registro. Después de habilitar el registro, AWS WAF envía los registros a través de Firehose a su destino de almacenamiento.

Para obtener información sobre cómo crear una Amazon Kinesis Data Firehose y revisar los registros almacenados, consulte ¿Qué es Amazon Data Firehose? Para conocer los permisos necesarios para la configuración de Kinesis Data Firehose, consulte Controlling Access with Amazon Kinesis Data Firehose.

Debe tener los siguientes permisos para habilitar el registro correctamente:

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `waf:PutLoggingConfiguration`

Para obtener más información acerca de los roles vinculados a servicios y el permiso `iam:CreateServiceLinkedRole`, consulte Uso de roles vinculados a servicios para Classic AWS WAF.

Para habilitar el registro para una ACL web

1. Cree una Amazon Kinesis Data Firehose con un nombre que comience con el aws-waf-logs prefijo "-» Por ejemplo,. `aws-waf-logs-us-east-2-analytics` Cree la instancia de Data Firehose con un origen PUT y en la región en la que opera. Si vas a capturar troncos para Amazon CloudFront, crea la manguera de incendios en EE. UU. Este (Norte de Virginia). Para obtener más información, consulte Creación de un flujo de entrega de Amazon Data Firehose.

   > **Important**
   >
   > No seleccione `Kinesis stream` como origen.
   > Un registro AWS WAF clásico equivale a un registro de Firehose. Si normalmente recibes 10 000 solicitudes por segundo y habilitas los registros completos, deberías tener una configuración de 10 000 registros por segundo en Firehose. Si no configuras Firehose correctamente, AWS WAF Classic no registrará todos los registros. Para obtener más información, consulte Cuotas de Amazon Kinesis Data Firehose.

2. Inicia sesión AWS Management Console y abre la AWS WAF consola en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.

3. En el panel de navegación, seleccione Web ACLs (ACL web).
4. Elija el nombre de la ACL web para la que desea habilitar el registro. Esto abre una página con los detalles de la ACL web en el panel derecho.
5. En la pestaña de Registro, elija Habilitar el registro.
6. Elija la instancia de Kinesis Data Firehose que creó en el primer paso. Debe elegir una manguera contra incendios que comience por "aws-waf-logs-».
7. (Opcional) Si no desea determinados campos y sus valores incluidos en los registros, redacte esos campos. Elija el campo que se va a redactar y, a continuación, elija Add (Añadir). Repita según sea necesario para redactar campos adicionales. Los campos redactados aparecen como `REDACTED` en los registros. Por ejemplo, si redacta el campo cookie (cookie), el campo cookie (cookie) de los registros será `REDACTED`.
8. Elija Enable logging (Habilitar el registro).

> **Note**
>
> Cuando habilite correctamente el registro, AWS WAF Classic creará un rol vinculado al servicio con los permisos necesarios para escribir registros en Amazon Kinesis Data Firehose. Para obtener más información, consulte Uso de roles vinculados a servicios para Classic AWS WAF.

Para deshabilitar el registro para una ACL web

1. En el panel de navegación, seleccione Web ACLs (ACL web).
2. Elija el nombre de la ACL web para la que desea deshabilitar el registro. Esto abre una página con los detalles de la ACL web en el panel derecho.
3. En la pestaña de Logging (registro), elija Disable logging (Deshabilitar el registro).
4. En el cuadro de diálogo, elija Disable logging (Deshabilitar el registro).

Example Registro de ejemplo


```
{

 "timestamp":1533689070589,
 "formatVersion":1,
 "webaclId":"385cb038-3a6f-4f2f-ac64-09ab912af590",
 "terminatingRuleId":"Default_Action",
 "terminatingRuleType":"REGULAR",
 "action":"ALLOW",
 "httpSourceName":"CF",
 "httpSourceId":"i-123",
 "ruleGroupList":[
                         {
                          "ruleGroupId":"41f4eb08-4e1b-2985-92b5-e8abf434fad3",
                          "terminatingRule":null,
                          "nonTerminatingMatchingRules":[
                                                          {"action" : "COUNT",
                                                          "ruleId" :
 "4659b169-2083-4a91-bbd4-08851a9aaf74"}
                                                         ],
                          "excludedRules":               [
```

```
                                                          {"exclusionType" :
 "EXCLUDED_AS_COUNT",
                                                           "ruleId" :
 "5432a230-0113-5b83-bbb2-89375c5bfa98"}
                                                         ]
                         }
                        ],

 "rateBasedRuleList":[
                             {
                              "rateBasedRuleId":"7c968ef6-32ec-4fee-96cc-51198e412e7f",

                              "limitKey":"IP",
                              "maxRateAllowed":100

                             },
                             {
                              "rateBasedRuleId":"462b169-2083-4a93-bbd4-08851a9aaf30",
                              "limitKey":"IP",
                              "maxRateAllowed":100
                              }
                              ],

 "nonTerminatingMatchingRules":[
                                      {"action" : "COUNT",

                                       "ruleId" : "4659b181-2011-4a91-
bbd4-08851a9aaf52"}
                                     ],

 "httpRequest":{
                      "clientIp":"192.10.23.23",

                      "country":"US",

                      "headers":[

                                 {
                                  "name":"Host",
                                  "value":"127.0.0.1:1989"
                                 },
                                 {
                                  "name":"User-Agent",
                                  "value":"curl/7.51.2"
```

```
                                    },
                                    {
                                     "name":"Accept",
                                     "value":"*/*"
                                    }
                                  ],
                        "uri":"REDACTED",
                        "args":"usernam=abc",
                        "httpVersion":"HTTP/1.1",
                        "httpMethod":"GET",
                        "requestId":"cloud front Request id"
                        }
}
```

A continuación verá una explicación de cada elemento incluido en estos registros:

Marca de tiempo

La marca de tiempo en milisegundos.

formatVersion

La versión de formato para el registro.

webaclId

El GUID de la ACL web.

terminatingRuleId

El ID de la regla que terminó la solicitud. Si nada termina la solicitud, el valor es `Default_Action`.

terminatingRuleType

El tipo de regla que terminó la solicitud. Valores posibles: RATE_BASED, REGULAR y GROUP.

acción

La acción. Valores posibles para una regla de terminación: ALLOW y BLOCK. COUNT no es un valor válido para una regla de terminación.

terminatingRuleMatchDetalles

Información detallada sobre la regla de finalización que coincide con la solicitud. Una regla de finalización tiene una acción que finaliza el proceso de inspección ante una solicitud web. Las

acciones posibles para una regla de terminación son ALLOW y BLOCK. Esto solo se rellena para las instrucciones de reglas de coincidencia de inyección de código SQL y scripting entre sitios (XSS). Al igual que sucede con todas las declaraciones de reglas que inspeccionan más de un aspecto, AWS WAF aplica la acción en la primera coincidencia y deja de inspeccionar la solicitud web. Una solicitud web con una acción de terminación podría contener otras amenazas, además de la indicada en el registro.

httpSourceName

El origen de la solicitud. Valores posibles: CF (si la fuente es Amazon CloudFront), APIGW (si la fuente es Amazon API Gateway) y ALB (si la fuente es un Application Load Balancer).

httpSourceId

El ID de origen. Este campo muestra el ID de la CloudFront distribución de Amazon asociada, la API REST de API Gateway o el nombre de un Application Load Balancer.

ruleGroupList

La lista de grupos de reglas que actuaron en esta solicitud. En el ejemplo de código anterior, solo aparece uno.

ruleGroupId

El ID del grupo de reglas. Si la regla bloqueó la solicitud, el ID de `ruleGroupID` es el mismo que el ID de `terminatingRuleId`.

terminatingRule

La regla del grupo de reglas que terminó la solicitud. Si este es un valor distinto de NULL, también contiene un ruleid (id de regla) y una action (acción). En este caso, la acción siempre es BLOCK.

nonTerminatingMatchingReglas

La lista de reglas del grupo de reglas que coinciden con la solicitud. Siempre son reglas COUNT (reglas coincidentes que no son de terminación).

acción (grupo de nonTerminatingMatching reglas)

Siempre es COUNT (reglas coincidentes que no son de terminación).

RuleID nonTerminatingMatching (grupo de reglas)

El ID de la regla del grupo de reglas que coincide con la solicitud y no era de terminación. Es decir, reglas COUNT.

excludedRules

La lista de reglas del grupo de reglas que ha excluido. La acción para estas reglas se establece en COUNT.

exclusionType (excludedRules group)

Un tipo que indica que la regla excluida tiene la acción COUNT.

ruleId (excludedRules group)

El ID de la regla del grupo de reglas que se ha excluido.

rateBasedRuleLista

La lista de reglas basadas en frecuencia que actuaron en la solicitud.

rateBasedRuleID

El ID de la regla basada en frecuencia que actuó en la solicitud. Si esto ha terminado la solicitud, el ID de `rateBasedRuleId` es el mismo que el ID de `terminatingRuleId`.

limitKey

El campo que se AWS WAF utiliza para determinar si es probable que las solicitudes provengan de una sola fuente y, por lo tanto, estén sujetas a un control de tarifas. Valor posible: IP.

maxRateAllowed

El número máximo de solicitudes, que tienen un valor idéntico en el campo especificado por `limitKey`, permitido en un periodo de cinco minutos. Si el número de solicitudes supera la regla `maxRateAllowed` y también se cumplen los demás predicados especificados en la regla, se AWS WAF activa la acción especificada para esta regla.

httpRequest

Los metadatos sobre la solicitud.

clientIp

La dirección IP del cliente que envía la solicitud.

country

El país de origen de la solicitud. Si AWS WAF no puede determinar el país de origen, establece este campo en. -

headers

La lista de encabezados.

uri

El URI de la solicitud. En el ejemplo de código anterior se muestra cuál sería el valor si este campo se hubiera ocultado.

args

La cadena de consulta.

httpVersion

La versión de HTTP.

httpMethod

El método HTTP en la solicitud.

ID de solicitud

El ID de la solicitud.

Enumeración de las direcciones IP bloqueadas por reglas basadas en frecuencia

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

AWS WAF La versión clásica proporciona una lista de direcciones IP que están bloqueadas por reglas basadas en tasas.

Para ver las direcciones IP bloqueadas por reglas basadas en frecuencia

1. Inicie sesión AWS Management Console y abra la AWS WAF consola en https://console.aws.amazon.com/wafv2/.

   Si ve Cambiar a la AWS WAF versión clásica en el panel de navegación, selecciónela.

2. En el panel de navegación, seleccione Reglas.
3. En la columna Name, elija una regla basada en frecuencia.

   La lista muestra las direcciones IP que la regla bloquea actualmente.

Cómo funciona AWS WAF Classic con las CloudFront funciones de Amazon

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debes usar esta versión si creaste AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los has migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Al crear una ACL web, puede especificar una o más CloudFront distribuciones que desea que AWS WAF Classic inspeccione. AWS WAF Classic comienza a permitir, bloquear o contar las solicitudes web para esas distribuciones en función de las condiciones que usted identifique en la ACL web. CloudFront proporciona algunas funciones que mejoran la funcionalidad AWS WAF clásica. En este capítulo se describen algunas formas que puede configurar CloudFront para que la AWS WAF versión clásica CloudFront y la versión clásica funcionen mejor juntas.

Temas

- Uso de AWS WAF Classic con páginas de error CloudFront personalizadas
- Uso de AWS WAF Classic with CloudFront para aplicaciones que se ejecutan en su propio servidor HTTP
- Elegir los métodos HTTP que CloudFront respondan a

Uso de AWS WAF Classic con páginas de error CloudFront personalizadas

Cuando AWS WAF Classic bloquea una solicitud web en función de las condiciones que especifiques, devuelve el código de estado HTTP 403 (Prohibido) a CloudFront. A continuación,

CloudFront devuelve ese código de estado al espectador. El visor muestra un breve mensaje predeterminado con formato elemental similar a este:

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

Si prefieres mostrar un mensaje de error personalizado, posiblemente con el mismo formato que el resto del sitio web, puedes configurarlo CloudFront para que devuelva al espectador un objeto (por ejemplo, un archivo HTML) que contenga el mensaje de error personalizado.

> **Note**
>
> CloudFront no puedes distinguir entre un código de estado HTTP 403 que devuelve tu origen y uno que devuelve AWS WAF Classic cuando se bloquea una solicitud. Esto significa que no puede devolver diferentes páginas de error personalizadas en función de las diferentes causas de un código de estado HTTP 403.

Para obtener más información sobre las páginas de error CloudFront personalizadas, consulte Personalización de las respuestas de error en la Guía para CloudFront desarrolladores de Amazon.

Uso de AWS WAF Classic with CloudFront para aplicaciones que se ejecutan en su propio servidor HTTP

Cuando utilizas AWS WAF Classic with CloudFront, puedes proteger las aplicaciones que se ejecutan en cualquier servidor web HTTP, ya sea un servidor web que se ejecute en Amazon Elastic Compute Cloud (Amazon EC2) o un servidor web que gestiones de forma privada. También puede configurarlo CloudFront para que requiera HTTPS entre CloudFront y su propio servidor web, así como entre los espectadores y. CloudFront

Requiere HTTPS entre CloudFront y su propio servidor web

Si necesita HTTPS entre su servidor web CloudFront y su propio servidor web, puede utilizar la función de origen CloudFront personalizado y configurar la política de protocolo de origen y los ajustes del nombre de dominio de origen para orígenes específicos. En tu CloudFront configuración, puedes especificar el nombre DNS del servidor junto con el puerto y el protocolo que quieres usar CloudFront para recuperar objetos de tu origen. También debe asegurarse de que el certificado SSL/TLS del servidor de origen personalizado coincide con el nombre de dominio de origen que ha configurado. Si utiliza su propio servidor web HTTP fuera de AWS, debe utilizar un certificado firmado

por una autoridad de certificación (CA) externa de confianza, por ejemplo, Comodo o Symantec DigiCert. Para obtener más información sobre cómo se requiere HTTPS para la comunicación entre CloudFront y su propio servidor web, consulte el tema Requerir HTTPS para la comunicación entre CloudFront y su origen personalizado en la Guía para CloudFront desarrolladores de Amazon.

Exigir HTTPS entre un espectador y CloudFront

Para requerir HTTPS entre los espectadores y CloudFront, puede cambiar la política de protocolo de visualización para uno o más comportamientos de caché en su CloudFront distribución. Para obtener más información sobre el uso de HTTPS entre espectadores CloudFront, consulte el tema Exigir HTTPS para la comunicación entre espectadores y CloudFront en la Guía para CloudFront desarrolladores de Amazon. También puedes traer tu propio certificado SSL para que los espectadores puedan conectarse a tu CloudFront distribución a través de HTTPS con tu propio nombre de dominio, por ejemplo, https://www.mysite.com. Para obtener más información, consulte el tema Configuración de nombres de dominio alternativos y HTTPS en la Guía para CloudFront desarrolladores de Amazon.

Elegir los métodos HTTP que CloudFront respondan a

Cuando creas una distribución CloudFront web de Amazon, eliges los métodos HTTP que quieres CloudFront procesar y reenviar a tu origen. Puede elegir entre las siguientes opciones:

- GET, HEAD: CloudFront solo puedes usarlos para obtener objetos de tu origen o para obtener encabezados de objetos.
- GET, HEAD, OPTIONS: CloudFront solo puedes usarlos para obtener objetos de tu origen, obtener encabezados de objetos o recuperar una lista de las opciones que admite tu servidor de origen.
- GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE: puedes utilizarlas CloudFront para obtener, añadir, actualizar y eliminar objetos, así como para obtener encabezados de objetos. Además, puede realizar otras operaciones de POST como enviar datos desde un formulario web.

También puede utilizar las condiciones AWS WAF clásicas de coincidencia de cadenas para permitir o bloquear las solicitudes basadas en el método HTTP, tal y como se describe enTrabajar con condiciones de coincidencia de cadena. Si desea utilizar una combinación de métodos CloudFront compatibles, como `GET` y`HEAD`, no necesita configurar AWS WAF Classic para bloquear las solicitudes que utilizan los demás métodos. Si desea permitir una combinación de métodos que CloudFront no sea compatible, por ejemplo, y `GET HEADPOST`, puede configurarla para que responda

CloudFront a todos los métodos y, a continuación, utilizar la AWS WAF versión clásica para bloquear las solicitudes que utilizan otros métodos.

Para obtener más información sobre cómo elegir los métodos CloudFront adecuados, consulte Métodos HTTP permitidos en el tema Valores que se especifican al crear o actualizar una distribución web de la Guía para CloudFront desarrolladores de Amazon.

Seguridad en AWS WAF Classic

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la versión más reciente. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad que se aplican a AWS WAF Classic, consulte AWS los servicios incluidos en el ámbito de aplicación por programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida al utilizar la AWS WAF versión clásica. Los siguientes temas muestran cómo configurar AWS WAF

Classic para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de AWS WAF Classic.

Temas

Protección de datos en AWS WAF Classic

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS WAF Classic. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para

cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con AWS WAF Classic o con otros dispositivos Servicios de AWS mediante la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

AWS WAF Las entidades clásicas (como las ACL web, las reglas y las condiciones) se cifran en reposo, excepto en determinadas regiones en las que el cifrado no está disponible, como China (Pekín) y China (Ningxia). Para cada región se utilizan claves de cifrado únicas.

Eliminar recursos clásicos AWS WAF

Puedes eliminar los recursos que crees en la AWS WAF versión clásica. Consulte las directrices para cada tipo de recurso en las siguientes secciones.

- Eliminación de una ACL web
- Añadir y eliminar reglas de un grupo de reglas AWS WAF clásico
- Eliminar una regla

Gestión de identidad y acceso para AWS WAF Classic

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar AWS WAF los recursos de la versión clásica. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que se realice en AWS WAF la versión clásica.

Usuario del servicio: si utiliza el servicio AWS WAF clásico para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más funciones AWS WAF clásicas para realizar su trabajo, es posible que necesite permisos

adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en AWS WAF Classic, consulte Solución de problemas de identidad y acceso AWS WAF clásicos.

Administrador de servicios: si está a cargo de los recursos de AWS WAF Classic en su empresa, probablemente tenga acceso completo a AWS WAF Classic. Su trabajo consiste en determinar a qué funciones y recursos de la AWS WAF versión clásica deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM con la AWS WAF versión clásica, consulteCómo funciona AWS WAF Classic con IAM.

Administrador de IAM: si es administrador de IAM, puede que le interese obtener más información sobre cómo redactar políticas para administrar el acceso a la versión clásica. AWS WAF Para ver ejemplos de políticas AWS WAF clásicas basadas en la identidad que puede utilizar en IAM, consulte. Ejemplos de políticas basadas en identidad para AWS WAF Classic

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS Single Sign-On y Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS Single Sign-On. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como

contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS Single Sign-On.
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.

- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, en algunos casos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de

instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad.

Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifique el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.

- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona AWS WAF Classic con IAM

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.

Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Antes de usar IAM para administrar el acceso a la AWS WAF versión clásica, infórmese sobre las funciones de IAM disponibles para su uso con AWS WAF la versión clásica.

Funciones de IAM que puede utilizar con la versión clásica AWS WAF

Característica de IAM	AWS WAF Soporte clásico
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan los AWS servicios AWS WAF clásicos y otros con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para la versión clásica AWS WAF

Compatibilidad con las políticas basadas en identidades	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Para ver ejemplos de políticas AWS WAF clásicas basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para AWS WAF Classic

Políticas basadas en recursos dentro de la versión clásica AWS WAF

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política

en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Acciones políticas para AWS WAF la versión clásica

Admite acciones de política	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones AWS WAF clásicas, consulte Acciones definidas por región AWS WAF y Acciones definidas por AWS WAF región en la Referencia de autorización de servicios.

En la AWS WAF versión clásica, las acciones políticas utilizan el siguiente prefijo antes de la acción:

```
waf
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "waf:action1",
      "waf:action2"
         ]
```

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones de la AWS WAF versión clásica que comiencen por`List`, incluya la siguiente acción:

```
"Action": "waf:List*"
```

Para ver ejemplos de políticas AWS WAF clásicas basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para AWS WAF Classic

Recursos de políticas para Classic AWS WAF

Admite recursos de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver la lista de tipos de recursos AWS WAF clásicos y sus ARN, consulte Recursos definidos por región AWS WAF y Recursos definidos por AWS WAF región en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS WAF y Acciones definidas por AWS WAF Regional. Para permitir o denegar el acceso a un subconjunto de recursos AWS WAF clásicos, incluya el ARN del recurso en el elemento de `resource` la política.

En la AWS WAF versión clásica, los recursos son reglas y ACL web. AWS WAF La versión clásica también admite condiciones como la coincidencia de bytes, la coincidencia de IP y la restricción de tamaño.

Estos recursos y condiciones tienen nombres de recursos de Amazon (ARN) únicos asociados a ellos, tal y como se muestra en la siguiente tabla:

Nombre en la consola AWS WAF	Nombre en AWS WAF SDK/CLI	Formato de ARN
ACL web	`WebACL`	`arn:aws:waf::` *`account`*`:`*`webacl`*`/`*`ID`
Regla	`Rule`	`arn:aws:waf::` *`account`*`:`*`rule`*`/`*`ID`
Condición de coincidencia de cadena	`ByteMatchSet`	`arn:aws:waf::` *`account`*`:`*`bytematchset`* `/`*`ID`
condición de coincidencia de inyección de código SQL	`SqlInjectionMatchSet`	`arn:aws:waf::` *`account`*`:`*`sqlinjectionset`* `/`*`ID`
Condición de restricción de tamaño	`SizeConstraintSet`	`arn:aws:waf::` *`account`*`:`*`sizeconstraintset`* `/`*`ID`
condición de coincidencia de IP	`IPSet`	`arn:aws:waf::` *`account`*`:`*`ipset`*`/`*`ID`
Condición de coincidencia de scripting entre sitios	`XssMatchSet`	`arn:aws:waf::` *`account`*`:`*`xssmatchset`* `/`*`ID`

Para permitir o denegar el acceso a un subconjunto de recursos AWS WAF clásicos, incluya el ARN del recurso en el elemento de `resource` la política. Los ARN de la AWS WAF versión clásica tienen el siguiente formato:

```
arn:aws:waf::account:resource/ID
```

Sustituya las variables *account*, *resource* e *ID* por valores válidos. Los valores válidos pueden ser los siguientes:

- *cuenta*: el ID de tu. Cuenta de AWS Debe especificar un valor.
- *recurso*: el tipo de recurso AWS WAF clásico.
- *ID*: el ID del recurso AWS WAF clásico o un comodín (*) para indicar todos los recursos del tipo especificado que están asociados al especificado Cuenta de AWS.

Por ejemplo, los siguientes ARN especifican todas las ACL web de la cuenta 111122223333:

```
arn:aws:waf::111122223333:webacl/*
```

Claves de condición de la política para la versión clásica AWS WAF

Admite claves de condición de políticas específicas del servicio	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación lógica `AND`. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición AWS WAF clásicas, consulte las claves de condición AWS WAF y los recursos definidos por AWS WAF región en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por región AWS WAF y Acciones definidas por AWS WAF región.

Para ver ejemplos de políticas AWS WAF clásicas basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para AWS WAF Classic

ACL en la versión clásica AWS WAF

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con Classic AWS WAF

Admite ABAC (etiquetas en las políticas)	Parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Classic AWS WAF

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para AWS WAF Classic

Admite Forward access sessions (FAS)	Sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción

en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio para AWS WAF Classic

Compatible con roles de servicio	Sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Si se cambian los permisos de un rol de servicio, es posible que se interrumpa la funcionalidad AWS WAF clásica. Edite las funciones de servicio solo cuando AWS WAF Classic proporcione instrucciones para hacerlo.

Funciones vinculadas al servicio para Classic AWS WAF

Compatible con roles vinculados al servicio	Sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre la creación o la administración de los roles AWS WAF clásicos vinculados a un servicio, consulte. Uso de roles vinculados a servicios para Classic AWS WAF

Ejemplos de políticas basadas en identidad para AWS WAF Classic

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos AWS WAF clásicos. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles, y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por AWS WAF Classic, incluido el formato de los ARN de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición para AWS WAF y Acciones, recursos y claves de condición para AWS WAF Regional en la Referencia de autorización de servicios.

Temas

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, eliminar o acceder a los recursos AWS WAF clásicos de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía del usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola clásica AWS WAF

Para acceder a la consola AWS WAF clásica, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos AWS WAF clásicos de su cuenta Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Los usuarios que pueden acceder a la AWS consola y utilizarla también pueden acceder a la consola AWS WAF clásica. No requieren otros permisos.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
```

```
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Solución de problemas de identidad y acceso AWS WAF clásicos

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la última versión. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con AWS WAF Classic e IAM.

Temas

- No estoy autorizado a realizar ninguna acción en Classic AWS WAF
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de la AWS WAF versión clásica

No estoy autorizado a realizar ninguna acción en Classic AWS WAF

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `waf:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 waf:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `waf:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibes un mensaje de error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferir un rol a AWS WAF Classic.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS WAF Classic. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de la AWS WAF versión clásica

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que

asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si AWS WAF Classic admite estas funciones, consulteCómo funciona AWS WAF Classic con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Uso de roles vinculados a servicios para Classic AWS WAF

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debes usar esta versión si creaste AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los has migrado a la versión más reciente. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

AWS WAF Classic utiliza funciones AWS Identity and Access Management vinculadas al servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Classic. AWS WAF AWS WAF Classic predefine los roles vinculados al servicio e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en tu nombre.

Un rol vinculado a un servicio facilita la configuración de AWS WAF Classic, ya que no es necesario añadir manualmente los permisos necesarios. AWS WAF Classic define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS WAF Classic puede asumir sus funciones. Los permisos definidos incluyen la política de confianza y la política de permisos. Dicha política de permisos no se puede asociar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a un servicio después de eliminar los recursos relacionados del rol. Esto protege sus recursos AWS WAF clásicos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a un servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de roles vinculados a servicios de AWS WAF Classic

AWS WAF Classic usa las siguientes funciones vinculadas a un servicio:

- `AWSServiceRoleForWAFLogging`
- `AWSServiceRoleForWAFRegionalLogging`

AWS WAF Classic usa estas funciones vinculadas a servicios para escribir registros en Amazon Data Firehose. Estas funciones solo se utilizan si habilita el inicio de sesión. AWS WAF Para obtener más información, consulte Registro de información del tráfico de la ACL web.

Los roles vinculados al servicio `AWSServiceRoleForWAFLogging` y `AWSServiceRoleForWAFRegionalLogging` confían en los siguientes servicios (respectivamente) para asumir el rol:

- `waf.amazonaws.com`

  `waf-regional.amazonaws.com`

Las políticas de permisos de las funciones permiten a AWS WAF Classic realizar las siguientes acciones en los recursos especificados:

- Acción: `firehose:PutRecord` y `firehose:PutRecordBatch` en Amazon Data Firehose, los recursos de transmisión de datos con un nombre que comience por «aws-waf-logs-». Por ejemplo, `aws-waf-logs-us-east-2-analytics`.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a servicios para AWS WAF Classic

No necesita crear manualmente un rol vinculado a servicios. Cuando habilita el AWS Management Console inicio de sesión AWS WAF clásico en la CLI AWS WAF clásica o la API AWS WAF clásica, AWS WAF Classic crea el rol vinculado al servicio automáticamente. `PutLoggingConfiguration`

Debe tener el permiso `iam:CreateServiceLinkedRole` para habilitar el registro.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al habilitar el registro AWS WAF clásico, AWS WAF Classic vuelve a crear el rol vinculado al servicio para usted.

Modificación de un rol vinculado a un servicio en instancias de AWS WAF Classic

AWS WAF La versión clásica no permite editar las funciones vinculadas a un servicio ni las funciones vinculadas al `AWSServiceRoleForWAFLogging` `AWSServiceRoleForWAFRegionalLogging` servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol utilizando IAM. Para más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM..

Eliminación de roles vinculados a servicios en AWS WAF Classic

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se monitorice ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el servicio AWS WAF clásico utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos AWS WAF clásicos utilizados por **`AWSServiceRoleForWAFLogging`** y **`AWSServiceRoleForWAFRegionalLogging`**

1. En la consola AWS WAF clásica, elimine el registro de todas las ACL web. Para obtener más información, consulte Registro de información del tráfico de la ACL web.
2. Mediante la API o la CLI, envíe una solicitud `DeleteLoggingConfiguration` para cada ACL web que tenga habilitado el registro. Para obtener más información, consulte la Referencia de la API de AWS WAF Classic.

Cómo eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la CLI de IAM o la API de IAM para eliminar los roles vinculados a servicios `AWSServiceRoleForWAFLogging` y `AWSServiceRoleForWAFRegionalLogging`. Para más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de AWS WAF Classic

AWS WAF La versión clásica admite el uso de funciones vinculadas a servicios en los siguientes casos. Regiones de AWS

Nombre de la región	Identidad de la región	Support en AWS WAF versión clásica
EE. UU. Este (Norte de Virginia)	`us-east-1`	Sí
EE. UU. Este (Ohio)	`us-east-2`	Sí
EE. UU Oeste (Norte de California)	`us-west-1`	Sí
Oeste de EE. UU. (Oregón)	`us-west-2`	Sí
Asia-Pacífico (Bombay)	`ap-south-1`	Sí

Nombre de la región	Identidad de la región	Support en AWS WAF versión clásica
Asia-Pacífico (Osaka)	ap-northeast-3	Sí
Asia-Pacífico (Seúl)	ap-northeast-2	Sí
Asia-Pacífico (Singapur)	ap-southeast-1	Sí
Asia-Pacífico (Sídney)	ap-southeast-2	Sí
Asia-Pacífico (Tokio)	ap-northeast-1	Sí
Canadá (centro)	ca-central-1	Sí
Europa (Fráncfort)	eu-central-1	Sí
Europa (Irlanda)	eu-west-1	Sí
Europa (Londres)	eu-west-2	Sí
Europa (París)	eu-west-3	Sí
América del Sur (São Paulo)	sa-east-1	Sí

Registro y supervisión en AWS WAF Classic

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la versión más reciente. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de AWS WAF Classic y sus AWS soluciones. Debe recopilar los datos de supervisión de todas las partes de la AWS solución para poder depurar más fácilmente un error multipunto en caso de que se produzca. AWS proporciona varias herramientas para supervisar los recursos de la AWS WAF versión clásica y responder a posibles eventos:

CloudWatch Alarmas Amazon

Al usar CloudWatch las alarmas, puede observar una única métrica durante un período de tiempo que especifique. Si la métrica supera un umbral determinado, CloudWatch envía una notificación a un tema o AWS Auto Scaling política de Amazon SNS. Para obtener más información, consulte Monitorización con Amazon CloudWatch.

AWS CloudTrail Registros

CloudTrail proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en la AWS WAF versión clásica. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a AWS WAF Classic, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales. Para obtener más información, consulte Registro de llamadas a la API de AWS CloudTrail con.

Validación de conformidad para AWS WAF Classic

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la versión más reciente. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Para saber si un programa de cumplimiento Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: este documento técnico describe cómo las empresas pueden crear aplicaciones aptas para AWS la HIPAA.

  > **Note**
  >
  > No Servicios de AWS todas cumplen los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.

- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde la perspectiva del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en lo AWS WAF clásico

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la versión más reciente. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

La infraestructura AWS global se basa en Regiones de AWS zonas de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Seguridad de infraestructura en AWS WAF Classic

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la versión más reciente. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

Como servicio gestionado, AWS WAF Classic está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a AWS WAF Classic a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

AWS WAF Cuotas clásicas

> **Note**
>
> Esta es la documentación de AWS WAF Classic. Solo debe usar esta versión si creó AWS WAF recursos, como reglas y ACL web, AWS WAF antes de noviembre de 2019 y aún no los ha migrado a la versión más reciente. Para migrar los recursos, consulte Migración de sus recursos AWS WAF clásicos a AWS WAF.
> Para obtener la versión más reciente de AWS WAF, consulteAWS WAF.

AWS WAF La versión clásica está sujeta a las siguientes cuotas (anteriormente denominadas límites).

AWS WAF Classic tiene cuotas predeterminadas en cuanto al número de entidades por cuenta y región. Puede solicitar un aumento de estas.

Recurso	Cuota predeterminada por cuenta y región
ACL de web	50
Reglas	100

Recurso	Cuota predeterminada por cuenta y región
R ate-based-rules	5
Condiciones por cuenta de y por región	Para todas las condiciones, excepto la coincidencia de expresiones regulares y la coincidencia geográfica, 100 de cada tipo de condición. Por ejemplo, 100 condiciones de restricción de tamaño y 100 condiciones de coincidencia de IP. Para ver las condiciones de coincidencia de expresiones regulares y geográficas, consulte la siguiente tabla.
Solicitudes por segundo	25 000 por ACL web*

*Esta cuota solo se aplica a AWS WAF Classic on an Application Load Balancer. Las cuotas de solicitudes por segundo (RPS) de AWS WAF Classic on CloudFront son las mismas CloudFront que las cuotas de RPS admitidas, tal como se describe en la Guía para desarrolladores. CloudFront

Las siguientes cuotas en las entidades AWS WAF clásicas no se pueden cambiar.

Recurso	Cuota por cuenta y región
Grupos de reglas por cada ACL web	2:1 grupo de reglas creado por el cliente y 1 AWS Marketplace grupo de reglas
Reglas por ACL web	10
Condiciones por regla	10
Rangos de direcciones IP (en notación CIDR) por condición de coincidencia IP	10 000 Puede actualizar hasta 1000 direcciones a la vez. La llamada a la API `UpdateIPSet` acepta un máximo de 1000 direcciones en una sola solicitud.
Direcciones IP bloqueadas por la regla basada en frecuencia	10 000
Límite mínimo de la regla basada en frecuencia en un periodo de cinco minutos	100

Recurso	Cuota por cuenta y región
Filtros por condición de coincidencia de scripting entre sitios	10
Filtros por condición de restricción de tamaño	10
Filtros por condición de coincidencia de inyección de código SQL	10
Filtros por condición de coincidencia de cadena	10
En condiciones de coincidencia de cadenas, el número de caracteres de los nombres de los encabezados HTTP, cuando se ha configurado AWS WAF Classic para inspeccionar los encabezados de las solicitudes web en busca de un valor específico	40
En condiciones de coincidencia de cadenas, el número de caracteres del valor que quieres que busque AWS WAF Classic	50
Condiciones de coincidencia de expresiones regulares	10
En condiciones de coincidencia de expresiones regulares, el número de caracteres del patrón que desea que AWS WAF busque Classic	70
En las condiciones de coincidencia de regex, el número de patrones por conjunto de patrones	10
En las condiciones de coincidencia de regex, el número de conjunto de patrones por condición regex	1
Conjuntos de patrones	5
Condiciones de coincidencia geográfica	50
Ubicaciones por condición de coincidencia geográfica	50

AWS WAF Classic tiene los siguientes cupos fijos de llamadas por cuenta y región. Estas cuotas se aplican al total de llamadas al servicio a través de cualquier medio disponible, incluida la consola, la CLI AWS CloudFormation, la API REST y los SDK. Estas cuotas no se pueden cambiar.

Tipo de llamada	Cuota por cuenta y región
Número máximo de llamadas a `AssociateWebACL`	Una solicitud cada dos segundos
Número máximo de llamadas a `DisassociateWebACL`	Una solicitud cada dos segundos
Número máximo de llamadas a `GetWebACLForResource`	Una solicitud por segundo
Número máximo de llamadas a `ListResourcesForWebACL`	Una solicitud por segundo
Número máximo de llamadas a `CreateWebACLMigrationStack`	Una solicitud por segundo
Número máximo de llamadas a `GetChangeToken`	10 solicitudes por segundo
Número máximo de llamadas a `GetChangeTokenStatus`	Una solicitud por segundo
Número máximo de llamadas a cualquier acción `List` individual, si no se define ninguna otra cuota.	5 solicitudes por segundo
Número máximo de llamadas a cualquier acción `Create`, `Put`, `Get` o `Update` individual, si no se define ninguna otra cuota.	Una solicitud por segundo

AWS Shield

La protección contra los ataques de denegación de servicio distribuido (DDoS) es de vital importancia para las aplicaciones con acceso a Internet. Al crear su aplicación AWS, puede hacer uso de las protecciones que se AWS proporcionan sin costo adicional. Además, puede utilizar el servicio de protección AWS Shield Advanced gestionada contra amenazas para mejorar su nivel de seguridad con funciones adicionales de detección, mitigación y respuesta a los ataques DDoS.

AWS se compromete a proporcionarle las herramientas, las mejores prácticas y los servicios que le ayudarán a garantizar una alta disponibilidad, seguridad y resiliencia en su defensa contra los actores maliciosos de Internet. Esta guía se facilita para ayudar a los responsables de la toma de decisiones de TI y a los ingenieros de seguridad a entender cómo utilizar Shield y Shield Advanced para proteger mejor sus aplicaciones de los ataques DDoS y otras amenazas externas.

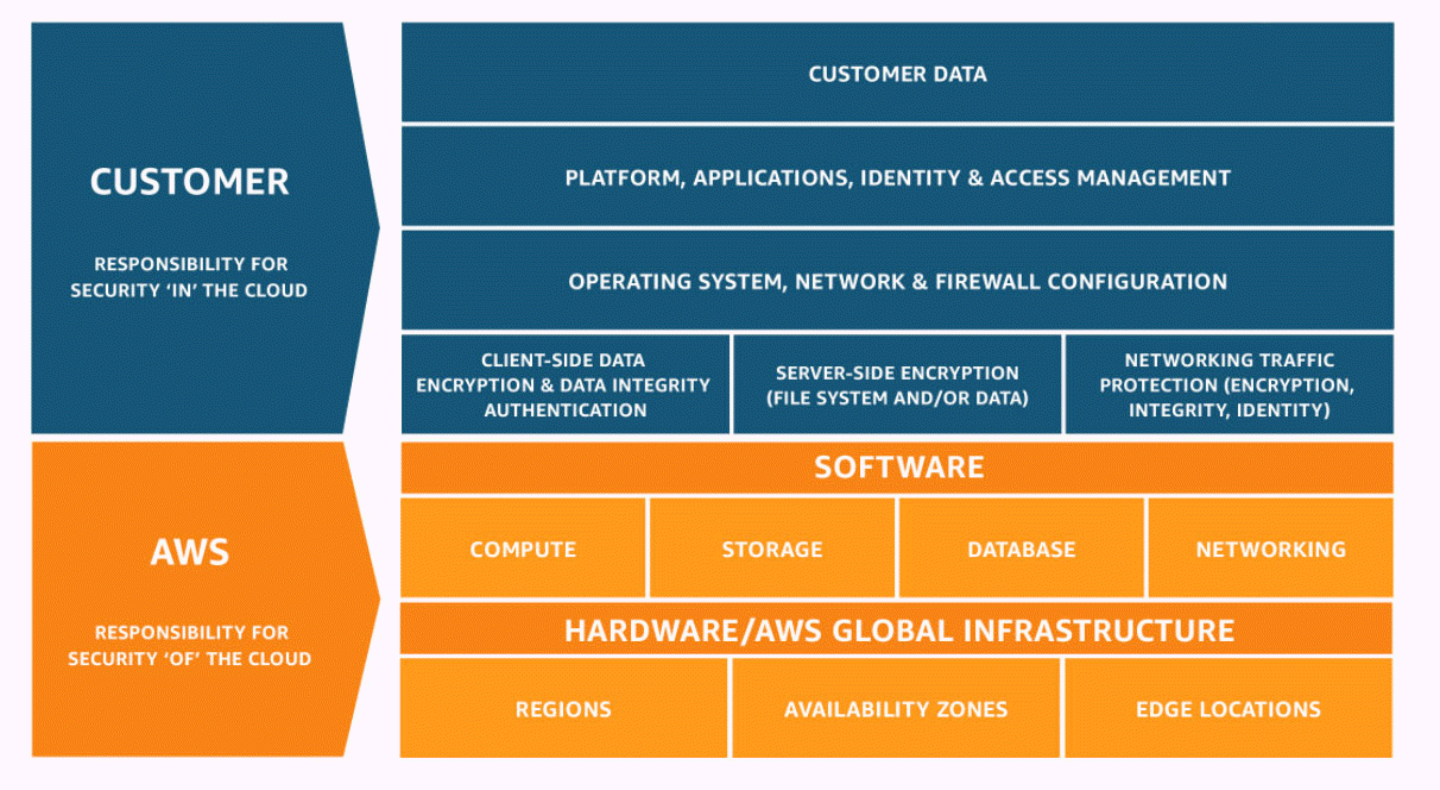
Cuando crea su aplicación AWS, recibe protección automática AWS contra los vectores de ataque DDoS volumétricos más comunes, como los ataques de reflexión UDP y las inundaciones de TCP SYN. Puede aprovechar estas protecciones para garantizar la disponibilidad de las aplicaciones en las que se ejecuta diseñando y AWS configurando su arquitectura para que sea resistente a los ataques DDoS.

Esta guía proporciona recomendaciones que pueden ayudarle a diseñar, crear y configurar las arquitecturas de sus aplicaciones para que sean resistentes a los ataques DDoS. Las aplicaciones que sigan las prácticas recomendadas en esta guía pueden beneficiarse de una mayor continuidad de la disponibilidad cuando sean objeto de ataques DDoS de mayor envergadura y de una gama más amplia de vectores de ataque DDoS. Además, esta guía le muestra cómo usar Shield Advanced para implementar un nivel de protección DDoS optimizado para sus aplicaciones esenciales. Estas incluyen las aplicaciones para las que ha garantizado un cierto nivel de disponibilidad para sus clientes y aquellas que requieren soporte operativo AWS durante los eventos de DDoS.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad que se aplican a Shield Advanced, consulte Servicios de AWS en el ámbito del programa de conformidad.

- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.



Cómo funcionan AWS Shield and Shield Advanced

AWS Shield Standard y AWS Shield Advanced proporcionan protección contra los ataques de denegación de servicio distribuido (DDoS) a AWS los recursos de las capas de red y transporte (capas 3 y 4) y de la capa de aplicaciones (capa 7). Un ataque DDoS es un ataque en el que varios sistemas comprometidos intentan inundar un objetivo con tráfico. Un ataque DDoS puede impedir que los usuarios finales legítimos accedan a los servicios de destino y puede provocar que el objetivo falle debido a un volumen de tráfico abrumador.

AWS Shield proporciona protección contra una amplia gama de vectores de ataque DDoS y vectores de ataque de día cero conocidos. La detección y mitigación de Shield están diseñadas para brindar cobertura contra las amenazas, incluso si el servicio no las conoce explícitamente en el momento de la detección. Shield Standard se proporciona automáticamente y sin costo adicional cuando se utiliza AWS.

Entre las clases de ataques que Shield detecta se incluyen las siguientes:

- Ataques volumétricos de red (capa 3): se trata de una subcategoría de los vectores de ataque a la capa de infraestructura. Estos vectores intentan saturar la capacidad de la red o el recurso objetivo para denegar el servicio a los usuarios legítimos.
- Ataques de protocolo de red (capa 4): se trata de una subcategoría de los vectores de ataque a la capa de infraestructura. Estos vectores abusan de un protocolo para denegar el servicio al recurso objetivo. Un ejemplo común de ataque a un protocolo de red es una inundación de TCP SYN, que puede agotar el estado de la conexión en recursos como servidores, equilibradores de carga o firewalls. Un ataque de protocolo de red también puede ser volumétrico. Por ejemplo, una inundación TCP SYN mayor puede tener como objetivo saturar la capacidad de una red y, al mismo tiempo, agotar el estado del recurso objetivo o de los recursos intermedios.
- Ataques a la capa de aplicación (capa 7): esta categoría de vector de ataque intenta denegar el servicio a los usuarios legítimos inundando una aplicación con consultas que son válidas para el objetivo, como las inundaciones de solicitudes web.

Contenido

- AWS Shield Advanced lógica de mitigación para aplicaciones web

AWS Shield Standard visión general

AWS Shield es un servicio gestionado de protección contra amenazas que protege el perímetro de su aplicación. El perímetro es el primer punto de entrada para el tráfico de aplicaciones que proviene de fuera de la AWS red.

Para determinar dónde se encuentra el perímetro de la aplicación, considere la forma en que los usuarios acceden a la aplicación desde Internet. Si el primer punto de entrada se encuentra en una AWS región, el perímetro de la aplicación es su Amazon Virtual Private Cloud (VPC). Si Amazon Route 53 dirige a los usuarios a su aplicación y primero acceden a la aplicación mediante Amazon CloudFront o AWS Global Accelerator, a continuación, el perímetro de la aplicación comienza en el extremo de la AWS red.

Shield proporciona beneficios de detección y mitigación de DDoS para todas las aplicaciones en las que se ejecutan AWS, pero las decisiones que tome al diseñar la arquitectura de la aplicación influirán en su nivel de resistencia a los DDoS. La resistencia a los ataques DDoS es la capacidad de su aplicación para seguir funcionando dentro de los parámetros esperados durante un ataque.

Todos AWS los clientes se benefician de la protección automática de Shield Standard, sin coste adicional. Shield Standard protege frente a los ataques DDoS más comunes que se suelen producir en la capa de red y transporte dirigidos contra su sitio web o sus aplicaciones. Si bien Shield Standard ayuda a proteger a todos AWS los clientes, usted obtiene beneficios especiales con las zonas alojadas de Amazon Route 53, CloudFront las distribuciones de Amazon y los aceleradores AWS Global Accelerator estándar. Estos recursos ofrecen una protección de disponibilidad integral contra todos los ataques conocidos a la capa de transporte y red.

AWS Shield Advanced visión general

AWS Shield Advanced es un servicio gestionado que le ayuda a proteger su aplicación contra amenazas externas, como los ataques DDoS, los bots volumétricos y los intentos de explotación de vulnerabilidades. Para obtener mayores niveles de protección contra ataques, puede suscribirse a AWS Shield Advanced.

Cuando se suscribe a Shield Advanced y añade protección a sus recursos, Shield Advanced ofrece una protección ampliada contra ataques DDoS para esos recursos. Las protecciones que reciba de Shield Advanced pueden variar en función de la arquitectura y las opciones de configuración. Utilice

la información de esta guía para crear y proteger aplicaciones resilientes con Shield Advanced y para ampliarlas cuando necesite la ayuda de un experto.

Suscripciones y AWS WAF costos de Shield Advanced

Su suscripción a Shield Advanced cubre los costes de uso de AWS WAF las capacidades estándar para los recursos que proteja con Shield Advanced. Las AWS WAF tarifas estándar que cubren las protecciones Shield Advanced son el costo por ACL web, el costo por regla y el precio base por millón de solicitudes de inspección de solicitudes web, hasta 1500 WCU y hasta el tamaño de cuerpo predeterminado.

Al habilitar la mitigación automática de DDoS en la capa de aplicaciones de Shield Advanced, se añade un grupo de reglas a la ACL web que utiliza 150 unidades de capacidad (WCU) de ACL web. Estas WCU se tienen en cuenta para el uso de la WCU en su ACL web. Para obtener más información, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced, El grupo de reglas de Shield Advanced y AWS WAF unidades de capacidad ACL web (WCU).

Su suscripción a Shield Advanced no cubre el uso AWS WAF de recursos que no proteja con Shield Advanced. Tampoco cubre ningún AWS WAF coste adicional no estándar de los recursos protegidos. Algunos ejemplos de AWS WAF costes no estándar son los del control de bots, la acción de la CAPTCHA regla, las ACL web que utilizan más de 1500 WCU y la inspección del cuerpo de la solicitud por encima del tamaño predeterminado. La lista completa se encuentra en la página de precios. AWS WAF

Para obtener la información completa y ejemplos de precios, consulte Precios de Shield y Precios de AWS WAF.

Facturación de suscripciones de Shield Advanced

Si eres un distribuidor de AWS canales, ponte en contacto con tu equipo de cuentas para obtener información y orientación. Esta información de facturación es para clientes que no son distribuidores de AWS canal.

Para todos los demás, se aplican las siguientes pautas de suscripción y facturación:

- En el caso de las cuentas que son miembros de una AWS Organizations organización, AWS factura las suscripciones de Shield Advanced a la cuenta de pagador de la organización, independientemente de si la propia cuenta de pagador está suscrita.
- Al suscribir varias cuentas que pertenezcan a la misma familia de cuentas de facturación de AWS Organizations consolidada, un único precio de suscripción cubre todas las cuentas suscritas de

la familia. La organización debe ser propietaria de todas las Cuentas de AWS y de todos sus recursos.

- Si suscribe varias cuentas para varias organizaciones, puede seguir pagando una única cuota de suscripción para todas las organizaciones, cuentas y recursos, siempre que sea el propietario de todos ellos. Póngase en contacto con su administrador de cuentas o con el servicio de AWS asistencia y solicite una exención de las tarifas de AWS Shield Advanced suscripción para todas las organizaciones excepto una.

Para obtener ejemplos e información detallada sobre precios, consulte Precios de AWS Shield.

Temas

- AWS Shield Advanced recursos protegidos
- AWS Shield Advanced capacidades y opciones
- Decidir si desea suscribirse a protecciones adicionales AWS Shield Advanced y aplicarlas

AWS Shield Advanced recursos protegidos

> **Note**
>
> Las protecciones de Shield Advanced solo están habilitadas para los recursos que haya especificado explícitamente en Shield Advanced o que proteja mediante una política de AWS Firewall Manager Shield Advanced. Shield Advanced no protege automáticamente sus recursos.

Puede usar Shield Advanced para una supervisión y protección avanzadas con los siguientes tipos de recursos:

- CloudFront Distribuciones de Amazon. Para CloudFront un despliegue continuo, Shield Advanced protege cualquier distribución provisional que esté asociada a una distribución principal protegida.
- Zonas alojadas de Amazon Route 53.
- AWS Global Accelerator aceleradores estándar.
- Direcciones IP elásticas de Amazon EC2. Shield Advanced protege los recursos asociados a las direcciones IP elásticas protegidas.
- Instancias de Amazon EC2, mediante la asociación a direcciones IP elásticas de Amazon EC2.

- Los siguientes equilibradores de carga Elastic Load Balancing (ELB):
  - Equilibradores de carga de aplicación.
  - Equilibradores de carga clásicos.
  - Equilibradores de carga de red, mediante asociaciones a direcciones IP elásticas de Amazon EC2.

Para obtener información adicional acerca de las protecciones para estos tipos de recursos, consulte AWS Shield Advanced protecciones por tipo de recurso.

AWS Shield Advanced capacidades y opciones

AWS Shield Advanced la suscripción incluye las siguientes capacidades y opciones. Estas funciones complementan las funciones de detección y mitigación de ataques DDoS que ya incluye. AWS

- AWS WAF integración: Shield Advanced utiliza ACL AWS WAF web, reglas y grupos de reglas como parte de las protecciones de la capa de aplicaciones. Para obtener más información al respecto AWS WAF, consulteCómo AWS WAF funciona.

> **Note**
>
> Su suscripción a Shield Advanced cubre los costes de uso de AWS WAF las capacidades estándar para los recursos que proteja con Shield Advanced. Las AWS WAF tarifas estándar que cubren las protecciones Shield Advanced son el costo por ACL web, el costo por regla y el precio base por millón de solicitudes de inspección de solicitudes web, hasta 1500 WCU y hasta el tamaño de cuerpo predeterminado.
> Al habilitar la mitigación automática de DDoS en la capa de aplicaciones de Shield Advanced, se añade un grupo de reglas a la ACL web que utiliza 150 unidades de capacidad (WCU) de ACL web. Estas WCU se tienen en cuenta para el uso de la WCU en su ACL web. Para obtener más información, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced, El grupo de reglas de Shield Advanced y AWS WAF unidades de capacidad ACL web (WCU).
> Su suscripción a Shield Advanced no cubre el uso AWS WAF de recursos que no proteja con Shield Advanced. Tampoco cubre ningún AWS WAF coste adicional no estándar de los recursos protegidos. Algunos ejemplos de AWS WAF costes no estándar son los del control de bots, la acción de la CAPTCHA regla, las ACL web que utilizan más de 1500 WCU y la inspección del cuerpo de la solicitud por encima del tamaño predeterminado. La lista completa se encuentra en la página de precios. AWS WAF

Para obtener la información completa y ejemplos de precios, consulte Precios de Shield y Precios de AWS WAF.

- Mitigación automática de DDoS en la capa de aplicación: puede configurar Shield Advanced para que responda automáticamente y mitigue los ataques de la capa de aplicaciones (capa 7) contra sus recursos protegidos. Con la mitigación automática, Shield Advanced impone límites AWS WAF de velocidad a las solicitudes de fuentes de DDoS conocidas y agrega y administra automáticamente AWS WAF protecciones personalizadas en respuesta a los ataques DDoS detectados. Puede configurar la mitigación automática para contar o bloquear las solicitudes web que forman parte de un ataque.

  Para obtener más información, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced.
- Detección basada en el estado: puede utilizar los controles de estado de Amazon Route 53 con Shield Advanced para informar sobre la detección y mitigación de eventos. Los controles de estado supervisan su aplicación de acuerdo con sus especificaciones y notifican que están en buen estado cuando se cumplen las especificaciones y en mal estado cuando no se cumplen. El uso de controles de estado con Shield Advanced ayuda a prevenir los falsos positivos y proporciona una detección y mitigación más rápidas cuando un recurso protegido no está en buen estado. Puede usar la detección basada en el estado para cualquier tipo de recurso, excepto para las zonas alojadas en Route 53. La participación proactiva de Shield Advanced solo está disponible para los recursos que tienen habilitada la detección basada en el estado.

  Para obtener más información, consulte Detección basada en la salud mediante controles de salud.
- Grupos de protección: puede usar los grupos de protección para crear agrupaciones lógicas de sus recursos protegidos, a fin de mejorar la detección y mitigación del grupo en su conjunto. Puede definir los criterios de pertenencia a un grupo de protección para que los recursos recién protegidos se incluyan automáticamente. Un recurso protegido puede pertenecer a varios grupos de protección.

  Para obtener más información, consulte AWS Shield Advanced grupos de protección.
- Visibilidad mejorada de los eventos y ataques de DDoS: Shield Advanced le brinda acceso a métricas e informes avanzados en tiempo real para obtener una amplia visibilidad de los eventos y ataques a sus recursos de AWS protegidos. Puedes acceder a esta información a través de la consola y la API Shield Advanced y a través de CloudWatch las métricas de Amazon.

Para obtener más información, consulte Visibilidad de los eventos de DDoS.

- Administración centralizada de las protecciones de Shield Advanced mediante AWS Firewall Manager: puede usar Firewall Manager para aplicar automáticamente las protecciones de Shield Advanced a sus nuevas cuentas y recursos y para implementar reglas de AWS WAF en sus ACL web. Las políticas de protección de Firewall Manager Shield Advanced se incluyen sin cargo adicional para los clientes de Shield Advanced. También puede centralizar las actividades de supervisión de Shield Advanced para sus cuentas mediante Firewall Manager con un tema de Amazon Simple Notification Service (SNS) o AWS Security Hub.

  Para obtener más información sobre el uso de Firewall Manager para administrar las protecciones de Shield Advanced, consulte AWS Firewall Manager y AWS Shield Advanced políticas. Para obtener información acerca de los precios de Firewall Manager, consulte Precios de AWS Firewall Manager.

- AWS Shield Response Team (SRT): La SRT tiene una amplia experiencia en la protección AWS de Amazon.com y sus subsidiarias. Como cliente de AWS Shield Advanced , puede ponerse en contacto con la SRT en cualquier momento para obtener ayuda durante un ataque DDoS que afecte a la disponibilidad de su aplicación. También puede trabajar con el SRT para crear y administrar mitigaciones personalizadas para sus recursos. Para utilizar los servicios del SRT, debe haberse suscrito al plan Business Support o en el plan Enterprise Support.

  Para obtener más información, consulte Asistencia del equipo de respuesta de Shield (Shield Response Team, SRT).

- Interacción proactiva: con la participación proactiva, el equipo de respuesta de Shield (SRT) se pone en contacto con usted directamente si la comprobación de estado de Amazon Route 53 que ha asociado a su recurso protegido deja de funcionar durante un evento detectado por Shield Advanced. Esto le permite interactuar con los expertos con rapidez cuando la disponibilidad de su aplicación pueda verse afectada por un ataque sospechoso.

  Para obtener más información, consulte Configuración de interacción proactiva.

- Oportunidades de protección de costos: Shield Advanced ofrece cierta protección de costos contra los picos en su AWS factura que podrían resultar de un ataque DDoS contra sus recursos protegidos. Esto puede incluir la cobertura de picos en las tarifas de uso de Shield Advanced Data Transfer Out (DTO). Shield Advanced ofrece cualquier tipo de protección de costos en forma de créditos de servicio Shield Advanced.

  Para obtener más información, consulte Solicitar un crédito en AWS Shield Advanced.

Decidir si desea suscribirse a protecciones adicionales AWS Shield Advanced y aplicarlas

Revise los escenarios de esta sección para ayudarte a decidir a qué cuentas suscribirse AWS Shield Advanced y dónde aplicar protecciones adicionales. Con Shield Advanced paga una cuota de suscripción mensual por todas las cuentas creadas en una cuenta de facturación unificada, más las tarifas de uso basadas en los GB de datos transferidos. Para obtener información sobre los precios de Shield Advanced, consulte Precios de AWS Shield Advanced.

Para proteger una aplicación y sus recursos con Shield Advanced, debe suscribir las cuentas que administran la aplicación a Shield Advanced y, a continuación, añadir protecciones a los recursos de la aplicación. Para obtener información sobre la suscripción de cuentas y la protección de los recursos, consulte Empezar con AWS Shield Advanced.

Suscripciones y AWS WAF costos de Shield Advanced

Su suscripción a Shield Advanced cubre los costes de uso de AWS WAF las capacidades estándar para los recursos que proteja con Shield Advanced. Las AWS WAF tarifas estándar que cubren las protecciones Shield Advanced son el costo por ACL web, el costo por regla y el precio base por millón de solicitudes de inspección de solicitudes web, hasta 1500 WCU y hasta el tamaño de cuerpo predeterminado.

Al habilitar la mitigación automática de DDoS en la capa de aplicaciones de Shield Advanced, se añade un grupo de reglas a la ACL web que utiliza 150 unidades de capacidad (WCU) de ACL web. Estas WCU se tienen en cuenta para el uso de la WCU en su ACL web. Para obtener más información, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced, El grupo de reglas de Shield Advanced y AWS WAF unidades de capacidad ACL web (WCU).

Su suscripción a Shield Advanced no cubre el uso AWS WAF de recursos que no proteja con Shield Advanced. Tampoco cubre ningún AWS WAF coste adicional no estándar de los recursos protegidos. Algunos ejemplos de AWS WAF costes no estándar son los del control de bots, la acción de la CAPTCHA regla, las ACL web que utilizan más de 1500 WCU y la inspección del cuerpo de la solicitud por encima del tamaño predeterminado. La lista completa se encuentra en la página de precios. AWS WAF

Para obtener la información completa y ejemplos de precios, consulte Precios de Shield y Precios de AWS WAF.

Facturación de suscripciones de Shield Advanced

Si eres un distribuidor de AWS canales, ponte en contacto con tu equipo de cuentas para obtener información y orientación. Esta información de facturación es para clientes que no son distribuidores de AWS canal.

Para todos los demás, se aplican las siguientes pautas de suscripción y facturación:

- En el caso de las cuentas que son miembros de una AWS Organizations organización, AWS factura las suscripciones de Shield Advanced a la cuenta de pagador de la organización, independientemente de si la propia cuenta de pagador está suscrita.
- Al suscribir varias cuentas que pertenezcan a la misma familia de cuentas de facturación de AWS Organizations consolidada, un único precio de suscripción cubre todas las cuentas suscritas de la familia. La organización debe ser propietaria de todas las Cuentas de AWS y de todos sus recursos.
- Si suscribe varias cuentas para varias organizaciones, puede seguir pagando una única cuota de suscripción para todas las organizaciones, cuentas y recursos, siempre que sea el propietario de todos ellos. Póngase en contacto con su administrador de cuentas o con el servicio de AWS asistencia y solicite una exención de las tarifas de AWS Shield Advanced suscripción para todas las organizaciones excepto una.

Para obtener información detallada sobre precios, consulte Precios de AWS Shield.

Identificación de las aplicaciones que se deben proteger

Considere la posibilidad de implementar las protecciones Shield Advanced para las aplicaciones en las que necesite alguno de los siguientes requisitos:

- Disponibilidad garantizada para los usuarios de la aplicación.
- Acceso rápido a expertos en mitigación de DDoS si la aplicación se ve afectada por un ataque DDoS.
- Consciente de AWS que la aplicación podría verse afectada por un ataque DDoS y notifique a sus equipos de seguridad o de operaciones los ataques AWS y su intensificación.
- Los costos de la nube son predecibles, incluso cuando un ataque DDoS afecta al uso de los servicios de AWS .

Si una aplicación o sus recursos requieren alguno de los requisitos anteriores, considere la posibilidad de crear suscripciones para las cuentas relacionadas.

Identificación de los recursos que se deben proteger

Para cada cuenta suscrita, considere la posibilidad de añadir una protección Shield Advanced a cada recurso que tenga alguna de las siguientes características:

- El recurso está destinado a usuarios externos de Internet.
- El recurso está expuesto a Internet y también forma parte de una aplicación crítica. Tenga en cuenta todos los recursos expuestos, independientemente de si tiene la intención de que los usuarios de Internet accedan a ellos.
- El recurso está protegido por una ACL AWS WAF web.

Para obtener más información acerca de cómo crear y administrar protecciones para recursos, consulte Protecciones de recursos en AWS Shield Advanced.

Además, siga las recomendaciones de esta guía para garantizar que la arquitectura de su aplicación sea resistente a los ataques DDoS y que haya configurado correctamente las características de Shield Advanced para lograr una protección óptima.

Ejemplos de ataques DDoS

AWS Shield Advanced proporciona una protección ampliada contra muchos tipos de ataques.

En la lista siguiente se describen algunos tipos de ataques comunes:

Ataques de reflexión del protocolo de datagramas de usuario (UDP)

En un ataque de reflexión de UDP, el atacante puede suplantar el origen de una solicitud y usar el UDP para obtener una respuesta grande del servidor. El tráfico de red adicional dirigido hacia la dirección IP suplantada y atacada puede ralentizar el servidor de destino e impedir que los usuarios finales obtengan acceso a los recursos necesarios.

Inundación TCP SYN

La intención de un ataque de inundación TCP SYN es agotar los recursos disponibles de un sistema dejando las conexiones en un estado semiabierto. Al conectarse un usuario a un servicio TCP como un servidor web, el cliente envía un paquete TCP SYN. El servidor devuelve un reconocimiento y el cliente devuelve su propio reconocimiento, completando el protocolo de tres modos. En una inundación TCP SYN, nunca se devuelve el tercer reconocimiento, mientras que

el servidor permanece a la espera de una respuesta. Esto puede impedir que otros usuarios se conecten al servidor.

Inundación de consultas DNS

En una avalancha de consultas de DNS, un atacante utiliza varias consultas de DNS para agotar los recursos de un servidor DNS. AWS Shield Advanced puede ayudar a brindar protección contra los ataques de avalancha de consultas de DNS en los servidores DNS de Route 53.

Ataques de inundación HTTP o ruptura de la caché (capa 7)

Con una inundación HTTP, incluidas las inundaciones de `GET` y `POST`, un atacante envía varias solicitudes HTTP que parecen ser de un usuario real de la aplicación web. Los ataques de ruptura de la caché son un tipo de inundación HTTP que usa variaciones en la cadena de consulta de la solicitud HTTP que impiden el uso de contenido almacenado en caché con ubicación de borde y fuerza la distribución del contenido desde el servidor web de origen, lo que provoca una sobrecarga adicional y potencialmente perjudicial en el servidor web de origen.

Cómo AWS Shield detecta los eventos

AWS opera sistemas de detección a nivel de servicio para la AWS red y los AWS servicios individuales, a fin de garantizar que permanezcan disponibles durante un ataque DDoS. Además, los sistemas de detección a nivel de recursos monitorean cada AWS recurso individual para garantizar que el tráfico hacia el recurso se mantenga dentro de los parámetros esperados. Esta combinación protege tanto el AWS recurso como los AWS servicios objetivo, al aplicar medidas de mitigación que descartan los paquetes defectuosos conocidos, destacan el tráfico potencialmente malicioso y priorizan el tráfico de los usuarios finales.

Los eventos detectados aparecen en los resúmenes de eventos, los detalles de los ataques y CloudWatch las métricas de Amazon de Shield Advanced como el nombre del vector de ataque DDoS o como `Volumetric` si la evaluación se hubiera basado en el volumen de tráfico y no en la firma. Para obtener más información sobre las dimensiones del vector de ataque que están disponibles en la `DDoSDetected` CloudWatch métrica, consulte AWS Shield Advanced métricas

Temas

- Lógica de detección de las amenazas en la capa de infraestructura
- Lógica de detección de amenazas en la capa de aplicación
- Lógica de detección para varios recursos en una aplicación

Lógica de detección de las amenazas en la capa de infraestructura

La lógica de detección utilizada para proteger AWS los recursos objetivo contra los ataques DDoS en las capas de infraestructura (capa 3 y capa 4) depende del tipo de recurso y de si el recurso está protegido con AWS Shield Advancedél.

Detección para Amazon CloudFront y Amazon Route 53

Cuando suministra su aplicación web con CloudFront Route 53, todos los paquetes que llegan a la aplicación son inspeccionados por un sistema de mitigación de DDoS totalmente integrado, que no introduce ninguna latencia observable. Los ataques DDoS contra CloudFront las distribuciones y las zonas alojadas en Route 53 se mitigan en tiempo real. Estas protecciones se aplican independientemente de si utiliza o no AWS Shield Advanced.

Siga la práctica recomendada de utilizar CloudFront Route 53 como punto de entrada de su aplicación web siempre que sea posible para detectar y mitigar los eventos de DDoS con la mayor rapidez.

Detección para AWS Global Accelerator servicios regionales

La detección a nivel de recursos protege los aceleradores y recursos AWS Global Accelerator estándar que se lanzan en AWS las regiones, como los balanceadores de carga clásicos, los balanceadores de carga de aplicaciones y las direcciones IP elásticas (EIP). Estos tipos de recursos se supervisan para detectar un aumento del tráfico que pueda indicar la presencia de un ataque DDoS que deba mitigarse. Cada minuto, se evalúa el tráfico de cada recurso de AWS . Si el tráfico en un recurso es elevado, se realizan comprobaciones adicionales para medir la capacidad del recurso.

Shield realiza las siguientes comprobaciones estándar:

- Instancias de Amazon Elastic Compute Cloud (Amazon EC2), EIP asociados a instancias de Amazon EC2: Shield recupera la capacidad del recurso protegido. La capacidad depende del tipo de instancia del objetivo, del tamaño de la instancia y de otros factores, como si la instancia utiliza una red mejorada.
- Equilibradores de carga clásicos y equilibradores de carga de aplicaciones: Shield recupera la capacidad del nodo del equilibrador de carga objetivo.
- EIP asociados a equilibradores de carga de red: Shield recupera la capacidad del equilibrador de carga objetivo. La capacidad es independiente de la configuración del grupo del equilibrador de carga objetivo.

- AWS Global Accelerator aceleradores estándar: Shield recupera la capacidad, que se basa en la configuración del punto final.

Estas evaluaciones se realizan en varias dimensiones del tráfico de la red, como el puerto y el protocolo. Si se excede la capacidad del recurso objetivo, Shield aplica una mitigación de DDoS. Las mitigaciones implementadas por Shield reducirán el tráfico DDoS, pero es posible que no lo eliminen. Shield también puede realizar una mitigación si se excede una fracción de la capacidad del recurso en una dimensión de tráfico coherente con los vectores de ataque DDoS conocidos. Shield efectúa esta mitigación con un tiempo de vida limitado (TTL), que se prolonga mientras el ataque continúe.

> **Note**
>
> Las mitigaciones implementadas por Shield reducirán el tráfico DDoS, pero puede que no lo eliminen. Puede aumentar Shield con soluciones como AWS Network Firewall o un firewall en el host iptables para evitar que su aplicación procese el tráfico que no es válido para su aplicación o que no fue generado por usuarios finales legítimos.

Las protecciones de Shield Advanced agregan lo siguiente a las actividades de detección de Shield existentes:

- Umbrales de detección más bajos: Shield Advanced sitúa las mitigaciones a mitad de la capacidad calculada. Esto puede proporcionar una mitigación más rápida de los ataques que se intensifican lentamente y de los ataques que tienen una firma volumétrica más ambigua.
- Protección contra ataques intermitentes: Shield Advanced asigna a las mitigaciones un tiempo de vida (TTL) que aumenta exponencialmente en función de la frecuencia y la duración de los ataques. Esto mantiene las mitigaciones durante más tiempo cuando se ataca un recurso con frecuencia y cuando un ataque se produce en ráfagas cortas.
- Detección basada en estado: al asociar una comprobación de estado de Route 53 a un recurso protegido de Shield Advanced, el estado de la comprobación de estado se utiliza en la lógica de detección. Durante un evento detectado, si la comprobación de estado es buena, Shield Advanced requiere mayor confianza en que se trata de un ataque antes de aplicar una mitigación. Si, por el contrario, la comprobación de estado no es buena, Shield Advanced podría aplicar una medida de corrección incluso antes de que se haya establecido la confianza. Esta característica ayuda a evitar los falsos positivos y proporciona una reacción más rápida ante los ataques que afectan a la aplicación. Para obtener información sobre las comprobaciones de estado con Shield Advanced, consulte Detección basada en la salud mediante controles de salud.

Lógica de detección de amenazas en la capa de aplicación

AWS Shield Advanced proporciona detección de capas de aplicaciones web para CloudFront distribuciones de Amazon protegidas y balanceadores de carga de aplicaciones. Cuando protege estos tipos de recursos con Shield Advanced, puede asociar una ACL web de AWS WAF con su protección para activar la detección de la capa de aplicaciones web. Shield Advanced consume los datos de solicitud de la ACL web asociada y crea una línea base de tráfico para su aplicación. La detección de la capa de aplicaciones web se basa en la integración nativa entre Shield Advanced y AWS WAF. Para obtener más información sobre las protecciones de la capa de aplicaciones, incluida la asociación de una ACL AWS WAF web a un recurso protegido de Shield Advanced, consulteAWS Shield Advanced protecciones de capa de aplicación (capa 7).

Para la detección de la capa de aplicaciones web, Shield Advanced monitorea el tráfico de las aplicaciones y lo compara con las líneas de base históricas en busca de anomalías. Este monitoreo cubre el volumen y la composición del tráfico totales. Durante un ataque DDoS, esperamos que cambien tanto el volumen como la composición del tráfico y Shield Advanced exige una desviación estadísticamente significativa en ambos para declarar un evento.

Shield Advanced realiza sus mediciones en función de ventanas temporales históricas. Este enfoque reduce las notificaciones de falsos positivos derivadas de cambios legítimos en el volumen de tráfico o de cambios en el tráfico que coinciden con un patrón esperado, como una venta que se ofrece a la misma hora todos los días.

> **Note**
>
> Evite los falsos positivos en sus protecciones de Shield Advanced dándole tiempo a Shield Advanced para establecer líneas de base que representen patrones de tráfico normales y legítimos. Shield Advanced comienza a recopilar información para su base de referencia al asociar una ACL web a su recurso protegido. Asocie una ACL web a su recurso protegido al menos 24 horas antes de cualquier evento planificado que pueda provocar patrones inusuales en el tráfico web. La detección de la capa de aplicaciones web de Shield Advanced es más precisa cuando ha observado 30 días de tráfico normal.

El tiempo que Shield Advanced tarda en detectar un evento depende del cambio que observe en el volumen de tráfico. En el caso de cambios de menor volumen, Shield Advanced observa el tráfico durante un período más prolongado para garantizar que se esté produciendo un evento. Para

cambios de volumen más elevados, Shield Advanced detecta e informa de un evento con mayor rapidez.

Una regla basada en la velocidad en su ACL web, ya sea que la agregue usted o la función de mitigación automática de la capa de aplicación Shield Advanced, puede mitigar un ataque antes de que alcance un nivel detectable. Para obtener más información sobre la mitigación automática de DDoS en la capa de aplicación, consulte. Mitigación de DDoS de la capa de aplicación automática de Shield Advanced

> **Note**
>
> Puede diseñar su aplicación para escalar en respuesta a un tráfico o una carga elevados a fin de garantizar que no se vea afectada por avalanchas de solicitudes más pequeñas. Con Shield Advanced, sus recursos protegidos están cubiertos por una protección de costos. Esto le ayuda a protegerse de los aumentos inesperados en su factura de servicios en la nube que podrían producirse como consecuencia de un ataque DDoS. Para obtener más información sobre la protección de costos de Shield Advanced, consulte Solicitar un crédito en AWS Shield Advanced.

Lógica de detección para varios recursos en una aplicación

Puede usar grupos de AWS Shield Advanced protección para crear colecciones de recursos protegidos que formen parte de la misma aplicación. Puede elegir qué recursos protegidos desea colocar en un grupo o indicar que todos los recursos del mismo tipo se traten como un grupo. Por ejemplo, puede crear un grupo de todos los equilibradores de carga de aplicaciones. Al crear un grupo de protección, la detección de Shield Advanced agrega todo el tráfico de los recursos protegidos del grupo. Esto resulta útil si tiene muchos recursos, cada uno de los cuales tiene una cantidad pequeña de tráfico, pero con un volumen agregado grande. También puede usar grupos de protección para preservar las líneas base de las aplicaciones, en el caso de implementaciones azul/verde en las que el tráfico se transfiere entre recursos protegidos.

Puede optar por agregar el tráfico de su grupo de protección de una de las siguientes maneras:

- Suma: esta agregación combina todo el tráfico entre los recursos del grupo de protección. Puede usar esta agregación para asegurarse de que los recursos recién creados tengan una línea base existente y para reducir la sensibilidad de detección, lo que puede ayudar a evitar los falsos positivos.

- Media: esta agregación utiliza el promedio de todo el tráfico del grupo de protección. Puede usar esta agregación para aplicaciones en las que el tráfico entre los recursos es uniforme, como los equilibradores de carga.
- Máximo: esta agregación utiliza el tráfico más alto de cualquier recurso del grupo de protección. Puede usar esta agregación cuando hay varios niveles de una aplicación en un grupo de protección. Por ejemplo, puede tener un grupo de protección que incluya una CloudFront distribución, su origen de Application Load Balancer y los destinos de instancia Amazon EC2 de Application Load Balancer.

También puede usar grupos de protección para mejorar la velocidad a la que Shield Advanced aplica las mitigaciones, en el caso de ataques dirigidos a varias IP elásticas con acceso a Internet o a aceleradores estándar de AWS Global Accelerator . Cuando el objetivo es un recurso de un grupo de protección, Shield Advanced establece confianza para los demás recursos del grupo. Esto pone en alerta la detección de Shield Advanced y puede reducir el tiempo necesario para crear mitigaciones adicionales.

Para obtener más información acerca de los grupos de protección, consulte AWS Shield Advanced grupos de protección.

Cómo AWS Shield mitiga los eventos

La lógica de mitigación que protege su aplicación puede variar en función de la arquitectura de su aplicación. Cuando protege una aplicación web con Amazon CloudFront y Amazon Route 53, se beneficia de las mitigaciones específicas de los casos de uso de la web y el DNS y que protegen todo el tráfico de los servicios. Cuando el punto de entrada de su aplicación es un recurso que se ejecuta en una AWS región, la lógica de mitigación varía según el servicio, el tipo de recurso y el uso que haga del mismo. AWS Shield Advanced

AWS Los ingenieros de Shield desarrollan los sistemas de mitigación de DDoS y están estrechamente integrados con AWS los servicios. Los ingenieros tienen en cuenta aspectos de su arquitectura, como la capacidad y el estado de los recursos específicos. Los ingenieros de Shield supervisan continuamente la eficacia y el rendimiento de los sistemas de mitigación de DDoS y son capaces de responder rápidamente cuando se descubren o anticipan nuevas amenazas.

Puede diseñar su aplicación para que escale en respuesta a un tráfico o una carga elevados, a fin de garantizar que no se vea afectada por oleadas de solicitudes más pequeñas. Si utiliza Shield Advanced para proteger sus recursos, recibirá cobertura contra los aumentos inesperados en su factura de la nube que puedan producirse como resultado de un ataque DDoS.

Mitigaciones de la infraestructura

En el caso de los ataques a la capa de infraestructura, los sistemas de mitigación de AWS Shield DDoS están presentes en el límite de la AWS red y en las ubicaciones AWS periféricas. La colocación de varios niveles de controles de seguridad en toda la AWS infraestructura proporciona defense-in-depth a sus aplicaciones en la nube.

Shield mantiene sistemas de mitigación de DDoS en todos los puntos de entrada desde Internet. Cuando Shield detecta un ataque DDoS, para cada punto de entrada, redirige el tráfico a través de los sistemas de mitigación de DDoS en la misma ubicación. Esto no introduce ninguna latencia adicional observable y proporciona una capacidad de mitigación de más de 100 TeraBits por segundo (Tbps) en todas AWS las regiones y ubicaciones periféricas. Shield protege la disponibilidad de sus recursos sin redirigir el tráfico a centros de depuración externos o remotos, lo que podría aumentar la latencia.

- En el límite de la AWS red, para cualquier AWS servicio o recurso, los sistemas de mitigación de DDoS mitigan los ataques a la capa de infraestructura procedentes de Internet. Los sistemas realizan sus mitigaciones cuando así lo indica la detección de Shield o un ingeniero del equipo de respuesta de Shield (SRT).
- En las ubicaciones AWS periféricas, los sistemas de mitigación de DDoS inspeccionan continuamente todos los paquetes que se reenvían a CloudFront las distribuciones de Amazon y a las zonas alojadas en Amazon Route 53, independientemente de su origen. Cuando es necesario, los sistemas aplican mitigaciones diseñadas específicamente para el tráfico web y de DNS. Una ventaja adicional de usar Amazon CloudFront y Amazon Route 53 para proteger sus aplicaciones web es que los ataques DDoS se mitigan inmediatamente, sin necesidad de una señal de detección de Shield.

Mitigaciones en la capa de la aplicación

Shield Advanced proporciona mitigaciones de la capa de aplicaciones web para las CloudFront distribuciones de Amazon y los balanceadores de carga de aplicaciones en las que has activado las protecciones de Shield Advanced. Cuando habilita la protección, asocia una ACL AWS WAF web al recurso para permitir la detección de la capa de aplicaciones web. Además, tiene la opción de activar la mitigación automática de la capa de aplicaciones, lo que indica a Shield Advanced que administre las protecciones por usted durante un ataque DDoS.

Shield solo proporciona mitigaciones personalizadas para los ataques de la capa de aplicación a los recursos para los que ha activado Shield Advanced y la mitigación automática de la capa de

aplicación. Con la mitigación automática, Shield Advanced impone límites AWS WAF de velocidad a las solicitudes de fuentes de DDoS conocidas y agrega y administra automáticamente AWS WAF protecciones personalizadas en respuesta a los ataques DDoS detectados. Para obtener información detallada sobre las mitigaciones de este tipo, consulte Cómo administra Shield Advanced la mitigación automática.

Una regla basada en la velocidad de su ACL web, ya sea que la haya agregado usted o la haya agregado mediante la función de mitigación automática de la capa de aplicación Shield Advanced, puede mitigar un ataque antes de que alcance un nivel detectable. Para obtener más información sobre la detección, consulteLógica de detección de amenazas en la capa de aplicación.

Características de mitigación

Las principales características de la mitigación de AWS Shield DDoS son las siguientes:

- Validación de paquetes: esto garantiza que cada paquete inspeccionado se ajuste a la estructura esperada y sea válido para su protocolo. Las validaciones de protocolo compatibles incluyen IP, TCP (incluidos el encabezado y las opciones), UDP, ICMP, DNS y NTP.
- Listas de control de acceso (ACL) y modeladores: una ACL evalúa el tráfico en función de atributos específicos y descarta el tráfico coincidente o lo asigna a un modelador. El modelador limita la velocidad de paquetes para el tráfico coincidente y elimina el exceso de paquetes para contener el volumen que llega al destino. AWS Shield Los ingenieros de detección y Shield Response Team (SRT) pueden asignar tarifas específicas al tráfico esperado y asignar tarifas más restrictivas al tráfico con atributos que coincidan con los vectores de ataque DDoS conocidos. Los atributos que puede igualar una ACL incluyen el puerto, el protocolo, los indicadores TCP, la dirección de destino, el país de origen y los patrones arbitrarios de la carga útil del paquete.
- Puntuación de sospecha: utiliza el conocimiento que Shield tiene sobre el tráfico esperado para aplicar una puntuación a cada paquete. A los paquetes que se ajustan más a los patrones de tráfico conocidos como seguros se les asigna una puntuación de sospecha más baja. La observación de los atributos de tráfico conocidos como maliciosos puede aumentar la puntuación de sospecha de un paquete. Cuando es necesario limitar la tasa de los paquetes, Shield descarta primero los paquetes con puntuaciones de sospecha más altas. Esto ayuda a Shield a mitigar los ataques DDoS conocidos y de día cero y, al mismo tiempo, evitar los falsos positivos.
- Proxy TCP SYN: proporciona protección contra las inundaciones de TCP SYN al enviar cookies TCP SYN para desafiar las nuevas conexiones antes de permitir que pasen al servicio protegido. El proxy TCP SYN que proporciona Shield DDoS Mitigation no tiene estado, lo que le permite mitigar los mayores ataques de inundación TCP SYN conocidos sin agotar el estado. Esto se logra

mediante la integración con AWS los servicios para transferir el estado de la conexión en lugar de mantener un proxy continuo entre el cliente y el servicio protegido. El proxy TCP SYN está disponible actualmente en Amazon CloudFront y Amazon Route 53.

- Distribución de tasa: ajusta continuamente los valores del modelador por ubicación según el patrón de entrada del tráfico hacia un recurso protegido. Esto evita limitar la velocidad del tráfico de clientes que podrían no ingresar a la AWS red de manera uniforme.

AWS Shield lógica de mitigación para CloudFront y Route 53

La mitigación de DDoS de Shield inspecciona continuamente el tráfico de Route CloudFront 53. Estos servicios funcionan desde una red distribuida a nivel mundial de ubicaciones AWS periféricas que le proporcionan un amplio acceso a la capacidad de mitigación de DDoS de Shield y distribuyen su aplicación desde una infraestructura que está más cerca de sus usuarios finales.

- CloudFront— Las mitigaciones de DDoS de Shield solo permiten que el tráfico válido para las aplicaciones web pase al servicio. Esto proporciona protección automática contra muchos de los vectores de DDoS más comunes, como los ataques de reflexión UDP.

  CloudFront mantiene las conexiones persistentes con el origen de la aplicación, las inundaciones de TCP SYN se mitigan automáticamente mediante la integración con la función de proxy TCP SYN Shield y Transport Layer Security (TLS) finaliza en la periferia. Estas características combinadas garantizan que el origen de su aplicación solo reciba solicitudes web bien formadas y que esté protegida contra ataques DDoS de capa inferior, inundaciones de conexiones y abuso de TLS.

  CloudFront utiliza una combinación de direccionamiento del tráfico DNS y enrutamiento anycast. Estas técnicas mejoran la resiliencia de su aplicación al mitigar los ataques cerca del origen, aislar las fallas y garantizar el acceso a la capacidad necesaria para mitigar los ataques más grandes conocidos.
- Route 53: las mitigaciones de Shield solo permiten que las solicitudes de DNS válidas lleguen al servicio. Shield mitiga las inundaciones de consultas de DNS mediante una puntuación de sospecha que prioriza las consultas que se sabe que son seguras y deja de priorizar las consultas que contienen atributos de ataque DDoS sospechosos o conocidos.

  Route 53 utiliza la partición aleatoria para proporcionar un conjunto único de cuatro direcciones IP de resolución para cada zona alojada, tanto para IPv4 como para IPv6. Cada dirección IP corresponde a un subconjunto diferente de ubicaciones de Route 53. Cada subconjunto de

ubicaciones consta de servidores DNS autorizados que solo se superponen parcialmente con la infraestructura de cualquier otro subconjunto. Esto garantiza que si la consulta de un usuario falla por cualquier motivo, se atenderá correctamente al volver a intentarlo.

Route 53 usa el enrutamiento anycast para dirigir las consultas de DNS a la ubicación periférica más cercana, en función de la proximidad de la red. Anycast también distribuye el tráfico DDoS a muchas ubicaciones periféricas, lo que evita que los ataques se centren en una sola ubicación.

Además de la velocidad de mitigación, CloudFront Route 53 ofrece un amplio acceso a la capacidad distribuida a nivel mundial de Shield. Para aprovechar estas capacidades, utilice estos servicios como punto de entrada para sus aplicaciones web dinámicas o estáticas.

Para obtener más información sobre el uso CloudFront de Route 53 para proteger las aplicaciones web, consulte Cómo ayudar a proteger las aplicaciones web dinámicas contra los ataques DDoS mediante Amazon CloudFront y Amazon Route 53. Para obtener más información sobre el aislamiento de fallas en Route 53, consulte Un estudio de caso en el aislamiento global de fallas.

AWS Shield lógica de mitigación para AWS las regiones

Los recursos que se lanzan en AWS las regiones están protegidos por sistemas de mitigación de AWS Shield DDoS colocados mediante la detección a nivel de recursos de Shield. Los recursos regionales incluyen las IP elásticas (EIP), los equilibradores de carga clásicos y los equilibradores de carga de aplicaciones.

Antes de implementar una mitigación, Shield identifica el recurso objetivo y su capacidad. Shield utiliza la capacidad para determinar el tráfico total máximo que sus mitigaciones deberían permitir que se reenvíe al recurso. Las listas de control de acceso (ACL) y otros modeladores incluidos en la mitigación pueden reducir los volúmenes permitidos para parte del tráfico, por ejemplo, el tráfico que coincide con vectores de ataque DDoS conocidos o que no se espera que llegue en gran volumen. Esto limita aun más la cantidad de tráfico que permiten las mitigaciones para ataques de reflexión UDP o para tráfico TCP que tiene indicadores TCP SYN o FIN.

Shield determina la capacidad y coloca las mitigaciones de forma diferente para cada tipo de recurso.

- En el caso de una instancia Amazon EC2 o una EIP adjunta a una instancia de Amazon EC2, Shield calcula la capacidad en función del tipo de instancia y otros atributos de la instancia, como si la instancia tuviese habilitada la red mejorada.
- En el caso de un equilibrador de carga de aplicación o un equilibrador de carga clásico, Shield calcula la capacidad de forma individual para cada nodo objetivo del equilibrador de carga. Las

mitigaciones de ataques DDoS para estos recursos se proporcionan mediante una combinación de mitigaciones de DDoS de Shield y el escalado automático mediante el equilibrador de carga. Cuando el equipo de respuesta de Shield (SRT) emprende un ataque contra un recurso de equilibrador de carga de aplicación o un equilibrador de carga clásico, es posible que acelere el escalado como medida de protección adicional.

- Shield calcula la capacidad de algunos AWS recursos en función de la capacidad disponible de la AWS infraestructura subyacente. Estos tipos de recursos incluyen los balanceadores de carga de red (NLB) y los recursos que enrutan el tráfico a través de los balanceadores de carga de puerta de enlace o. AWS Network Firewall

> **Note**
>
> Proteja sus equilibradores de carga de red adjuntando EIP protegidos por Shield Advanced. Puede trabajar con SRT para crear mitigaciones personalizadas basadas en el tráfico esperado y la capacidad de la aplicación subyacente.

Cuando Shield aplica una mitigación, los límites de tasa iniciales que Shield define en la lógica de mitigación se aplican por igual a todos los sistemas de mitigación de DDoS de Shield. Por ejemplo, si Shield establece una mitigación con un límite de 100.000 paquetes por segundo (pps), inicialmente permitirá 100.000 pps en cada ubicación. Luego, Shield agrega continuamente métricas de mitigación para determinar la proporción real de tráfico y usa la proporción para adaptar el límite de tasa para cada ubicación. Esto evita los falsos positivos y garantiza que las mitigaciones no sean demasiado permisivas.

AWS Shield lógica de mitigación para aceleradores AWS Global Accelerator estándar

Las mitigaciones de Shield permitirán que solo el tráfico válido llegue a los puntos de conexión oyentes de un acelerador estándar de Global Accelerator. Los aceleradores estándar se implementan en todo el mundo y te proporcionan direcciones IP que puedes usar para enrutar el tráfico a AWS los recursos de cualquier AWS región. Los límites de tasa que Shield aplica para mitigar el Global Accelerator se basan en las capacidades de los recursos a los que el acelerador estándar dirige el tráfico. Shield aplica mitigaciones cuando el tráfico total supera la tasa determinada y también cuando se supera una fracción de esa tasa para vectores DDoS conocidos.

Cuando configura un acelerador estándar, define grupos de puntos de conexión para cada región de AWS a la que enrutará el tráfico de su aplicación. Cuando Shield coloca una mitigación, calcula

la capacidad de cada grupo de puntos de conexión y actualiza los límites de tasa en cada sistema de mitigación de DDoS de Shield en consecuencia. La tarifa varía para cada ubicación, según las suposiciones de Shield sobre cómo se enrutará el tráfico de Internet a sus AWS recursos. La capacidad de un grupo de puntos de conexión se calcula multiplicando la cantidad de recursos del grupo por la capacidad más baja de cualquier recurso del grupo. A intervalos regulares, Shield recalcula la capacidad de su aplicación y actualiza los límites de tasa según sea necesario.

> **Note**
>
> El uso de los controles de tráfico para cambiar el porcentaje de tráfico que se dirige a un grupo de puntos de conexión no cambia la forma en que Shield calcula o distribuye los límites de tasa a sus sistemas de mitigación de DDoS. Si usa controles de tráfico, configure sus grupos de puntos de conexión para que se reflejen entre sí en términos de tipo y cantidad de recursos. Esto ayuda a garantizar que la capacidad calculada por Shield sea representativa de los recursos que atienden el tráfico de su aplicación.

Para obtener más información sobre los grupos de puntos de conexión y los números de tráfico en Global Accelerator, consulte Grupos de puntos de conexión en aceleradores estándar de AWS Global Accelerator.

AWS Shield Advanced lógica de mitigación para IP elásticas

Al proteger una IP elástica (EIP) con AWS Shield Advanced, Shield Advanced mejora las mitigaciones que Shield aplica durante un evento de DDoS. Los sistemas de mitigación de DDoS Shield Advanced replican la configuración de ACL de red (NACL) para la subred pública a la que está asociada la EIP. Por ejemplo, si su NACL está configurada para bloquear todo el tráfico UDP, Shield Advanced combina esa regla con las mitigaciones colocadas por Shield.

Esta funcionalidad adicional puede ayudarle a evitar los riesgos de disponibilidad debido a un tráfico que no es válido para su aplicación. También puede usar las NACL para bloquear direcciones IP de origen individuales o rangos de CIDR de direcciones IP de origen. Esta puede ser una herramienta de mitigación útil para los ataques DDoS que no se distribuyen. También le permite administrar fácilmente sus propias listas de permitidos o bloquear las direcciones IP que no deberían comunicarse con su aplicación, sin tener que recurrir a la intervención de los ingenieros. AWS

AWS Shield Advanced lógica de mitigación para aplicaciones web

AWS Shield Advanced utiliza AWS WAF para mitigar los ataques a la capa de aplicaciones web. AWS WAF está incluido en Shield Advanced sin coste adicional.

Protección estándar de la capa de aplicación

Cuando proteges una CloudFront distribución de Amazon o un Application Load Balancer con Shield Advanced, puedes usar Shield Advanced para asociar una ACL AWS WAF web a tu recurso protegido, si aún no tienes una asociada. Si aún no ha configurado una ACL web, puede usar el asistente de consola de Shield Advanced para crear una y agregarle una regla basada en tasas. Una regla basada en tasas limita el número de solicitudes por intervalo de cinco minutos para cada dirección IP, lo que proporciona protecciones básicas contra inundación de solicitudes de la capa de aplicaciones web. Puede configurar la tasa, empezando tan bajo como 100. Para obtener más información, consulte Shield: ACL AWS WAF web de capa de aplicación avanzada y reglas basadas en tasas.

También puede utilizar el AWS WAF servicio para gestionar la ACL web. De este AWS WAF modo, puede ampliar la configuración de la ACL web para hacer cosas como inspeccionar componentes específicos de las solicitudes web para comprobar si coinciden con las cadenas o patrones, añadir un tratamiento personalizado de las solicitudes y las respuestas y compararlos con la geolocalización del origen de la solicitud. Para obtener más información sobre AWS WAF las reglas, consulte. AWS WAF reglas

Mitigación automática en la capa de aplicación

Para una protección mejorada, active la mitigación automática de la capa de aplicación Shield Advanced. Con esta opción, Shield Advanced mantiene una regla AWS WAF de limitación de velocidad para las solicitudes de fuentes de DDoS conocidas y proporciona mitigaciones personalizadas para los ataques DDoS detectados.

Cuando Shield Advanced detecta un ataque a un recurso protegido, intenta identificar una firma de ataque que aísle el tráfico de ataque del tráfico normal a su aplicación. Shield Advanced evalúa la firma del ataque identificada comparándola con los patrones de tráfico históricos del recurso que está siendo atacado, así como de cualquier otro recurso que esté asociado a la misma ACL web.

Si Shield Advanced determina que la firma del ataque aísla solo el tráfico implicado en el ataque DDoS, implementa la firma en AWS WAF las reglas de la ACL web asociada. Puede indicar a Shield Advanced que coloque mitigaciones que solo cuenten el tráfico con el que coinciden o que

lo bloqueen, y puede cambiar la configuración en cualquier momento. Cuando Shield Advanced determina que sus reglas de mitigación ya no son necesarias, las elimina de la ACL web. Para obtener más información sobre la mitigación de eventos de la capa de aplicaciones, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced.

Para obtener más información sobre las mitigaciones de la capa de aplicación de Shield Advanced, consulte AWS Shield Advanced protecciones de capa de aplicación (capa 7).

Ejemplos de arquitecturas resilientes a DDoS básicas

La resistencia a los ataques DDoS es la capacidad de la arquitectura de su aplicación para resistir los ataques de denegación de servicio distribuido (DDoS) y, al mismo tiempo, seguir atendiendo a los usuarios finales legítimos. Una aplicación muy resistente puede permanecer disponible durante un ataque con un impacto mínimo en las métricas de rendimiento, como los errores o la latencia. En esta sección se muestran algunos ejemplos de arquitecturas comunes y se describe cómo utilizar las capacidades de detección y mitigación de DDoS que proporciona AWS Shield Advanced para aumentar su resistencia a los DDoS.

Los ejemplos de arquitecturas de esta sección destacan los servicios de AWS que ofrecen las mayores ventajas de resistencia a los ataques DDoS para las aplicaciones implementadas. Algunas de las ventajas de los servicios destacados son las siguientes:

- Acceso a una capacidad de red distribuida a nivel mundial: los servicios Amazon CloudFront y Amazon Route 53 le proporcionan acceso a Internet y a la capacidad de mitigación de DDoS en toda la red perimetral AWS global. AWS Global Accelerator Esto resulta útil para mitigar los ataques volumétricos más grandes, que pueden alcanzar una escala de terabits. Puede ejecutar su aplicación en cualquier AWS región y utilizar estos servicios para proteger la disponibilidad y optimizar el rendimiento de sus usuarios legítimos.
- Protección contra los vectores de ataque DDoS en la capa de aplicación web: la mejor forma de mitigar los ataques DDoS en la capa de aplicación web es mediante una combinación de una escala de aplicaciones y un firewall de aplicaciones web (WAF). Shield Advanced utiliza registros de inspección de solicitudes web AWS WAF para detectar anomalías que se pueden mitigar automáticamente o mediante la colaboración con el equipo de respuesta de AWS Shield (SRT). La mitigación automática está disponible a través de reglas basadas en tasas de AWS WAF implementadas y también a través de la mitigación automática de DDoS en la capa de aplicaciones Shield Advanced.

Además de revisar estos ejemplos, revise y siga las prácticas recomendadas aplicables en Prácticas recomendadas para la resiliencia DDoS de AWS.

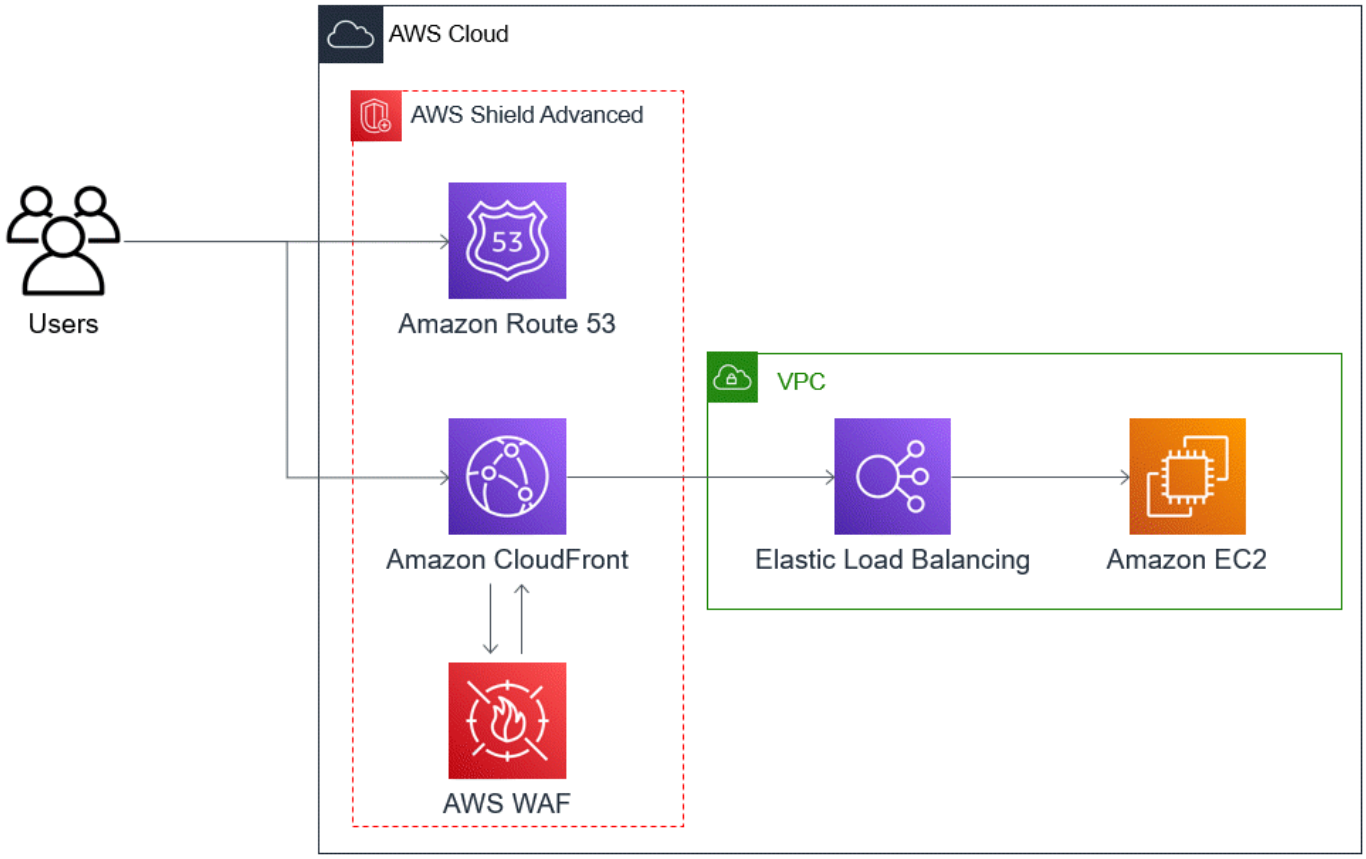
Ejemplo de resiliencia a DDoS para aplicaciones web comunes

Puede crear una aplicación web en cualquier AWS región y recibir protección automática contra ataques DDoS gracias a las funciones de detección y mitigación que AWS ofrece la región.

Este ejemplo es para arquitecturas que dirigen a los usuarios a una aplicación web mediante recursos como los Equilibradores de carga clásicos, Equilibradores de carga de aplicaciones, Equilibradores de carga de redes, soluciones Marketplace de AWS o su propia capa de proxy. Puede mejorar la resistencia a los ataques DDoS insertando zonas alojadas de Amazon Route 53, CloudFront distribuciones de Amazon y ACL AWS WAF web entre estos recursos de aplicaciones web y sus usuarios. Estas inserciones pueden ocultar el origen de la aplicación, atender las solicitudes más cerca de los usuarios finales y detectar y mitigar la avalancha de solicitudes en la capa de aplicaciones. Las aplicaciones que ofrecen contenido estático o dinámico a sus usuarios con Route 53 están protegidas por un sistema de mitigación de DDoS integrado CloudFront y totalmente integrado que mitiga los ataques a la capa de infraestructura en tiempo real.

Con estas mejoras arquitectónicas, podrá proteger sus zonas alojadas en Route 53 y sus CloudFront distribuciones con Shield Advanced. Al proteger CloudFront las distribuciones, Shield Advanced le pide que asocie las ACL AWS WAF web y cree reglas basadas en tasas para ellas, y le da la opción de habilitar la mitigación automática de DDoS en la capa de aplicación o la participación proactiva. La interacción proactiva y la mitigación automática de los ataques DDoS en la capa de aplicación utilizan las comprobaciones de estado de Route 53 que se asocian al recurso. Para más información sobre estas opciones, consulte Protecciones de recursos en AWS Shield Advanced.

El siguiente diagrama de referencia muestra esta arquitectura resistente a los ataques DDoS para una aplicación web.



Los beneficios que este enfoque proporciona a su aplicación web incluyen los siguientes:

- Protección contra los ataques DDoS de uso frecuente en la capa de infraestructura (capa 3 y capa 4), sin demora en la detección. Además, si un recurso es atacado con frecuencia, Shield Advanced coloca las mitigaciones durante períodos de tiempo más largos. Shield Advanced también utiliza el contexto de la aplicación deducido de las ACL de red (NACL) para bloquear el tráfico no deseado en sentido ascendente. Esto aísla las fallas más cerca de su origen, lo que minimiza el efecto en los usuarios legítimos.
- Protección contra las inundaciones de TCP SYN. Los sistemas de mitigación de DDoS integrados con CloudFront Route 53 AWS Global Accelerator ofrecen una función de proxy TCP SYN que desafía los nuevos intentos de conexión y solo sirven a los usuarios legítimos.
- Protección contra los ataques a la capa de aplicaciones del DNS, ya que Route 53 es responsable de ofrecer respuestas de DNS fiables.
- Protección contra las inundaciones de solicitudes en la capa de aplicaciones web. La regla basada en la velocidad que configuras en tu ACL AWS WAF web bloquea las IP de origen cuando envían más solicitudes de las que permite la regla.

- Mitigación automática de DDoS en la capa de aplicación para sus CloudFront distribuciones, si decide habilitar esta opción. Con la mitigación automática de DDoS, Shield Advanced mantiene una regla basada en la velocidad en la ACL AWS WAF web asociada a la distribución que limita el volumen de solicitudes de fuentes de DDoS conocidas. Asimismo, cuando Shield Advanced detecta un evento que afecta al estado de la aplicación, crea, prueba y administra automáticamente las reglas de mitigación en la ACL web.
- Interacción proactiva con el Shield Response Team (SRT), si decide habilitar esta opción. Cuando Shield Advanced detecta un evento que afecta al estado de su aplicación, el SRT responde e interactúa de forma proactiva con sus equipos de seguridad u operaciones utilizando la información de contacto que proporcione. El SRT analiza los patrones del tráfico y puede actualizar AWS WAF las reglas para bloquear el ataque.

Ejemplo de resiliencia DDoS para aplicaciones TCP y UDP

Este ejemplo muestra una arquitectura resistente a DDoS para aplicaciones TCP y UDP en una región de AWS que utiliza instancias de Amazon Elastic Compute Cloud (Amazon EC2) o direcciones IP elásticas (EIP).

Puede seguir este ejemplo general para mejorar la resistencia a los ataques DDoS para los siguientes tipos de aplicaciones:

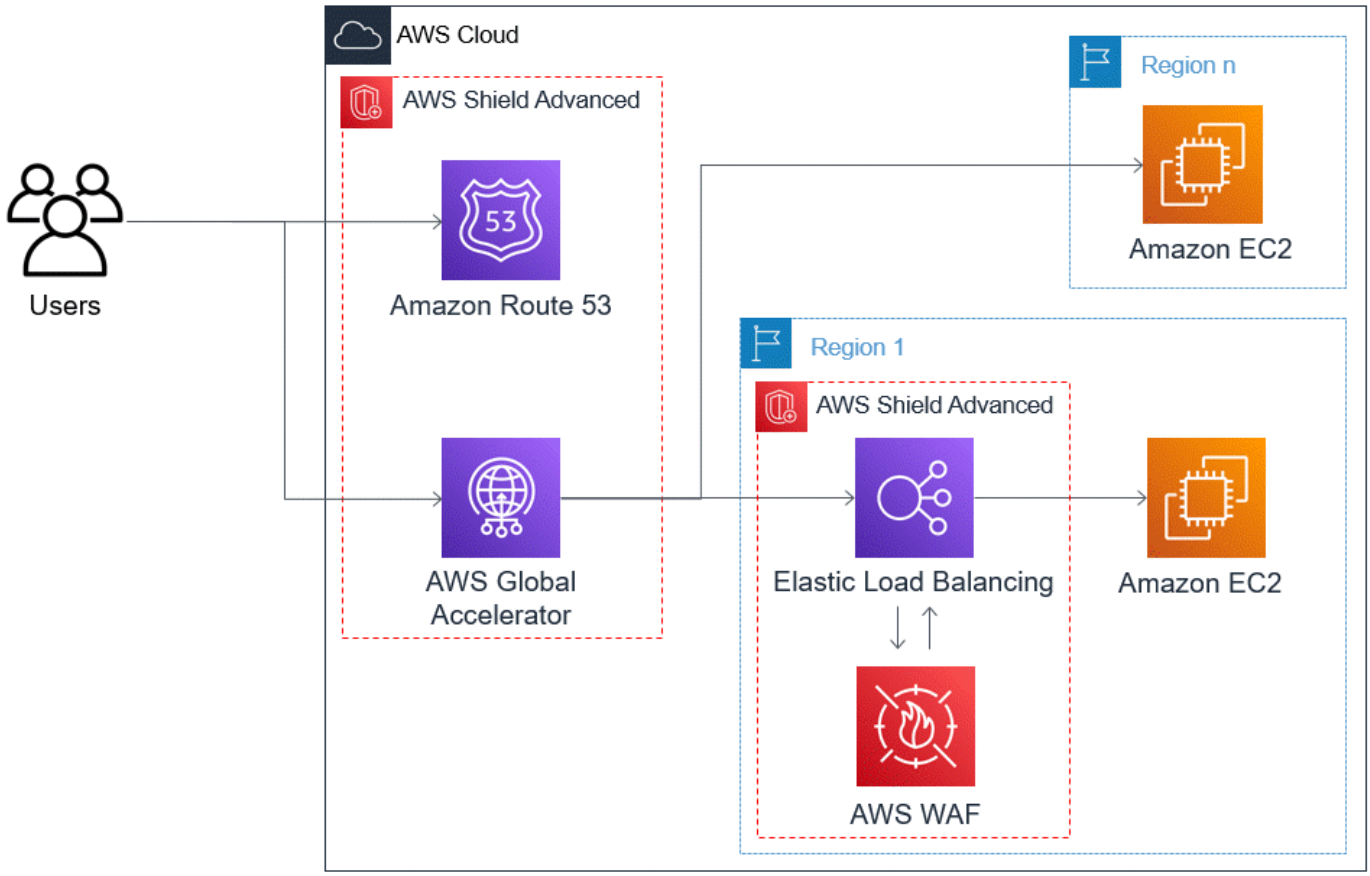
- Aplicaciones TCP o UDP. Por ejemplo, las aplicaciones utilizadas para juegos, IoT y voz sobre IP.
- Aplicaciones web que requieren direcciones IP estáticas o que utilizan protocolos que Amazon CloudFront no admite. Por ejemplo, es posible que tu aplicación requiera direcciones IP que los usuarios puedan añadir a sus listas de firewalls permitidas y que ningún otro AWS cliente utilice.

Puede mejorar la resistencia a los ataques DDoS de estos tipos de aplicaciones introduciendo Amazon Route 53 y AWS Global Accelerator. Estos servicios pueden dirigir a los usuarios a su aplicación y pueden proporcionar a su aplicación direcciones IP estáticas que se enrutan con el método anycast a través de la red perimetral global de AWS . Los aceleradores estándar de Global Accelerator pueden mejorar la latencia de los usuarios hasta en un 60 %. Si tiene una aplicación web, puede detectar y mitigar las inundaciones de solicitudes de la capa de aplicaciones web ejecutando la aplicación en un Application Load Balancer y, a continuación, protegiendo el Application Load Balancer con AWS WAF una ACL web.

Una vez que haya creado la aplicación, proteja las zonas alojadas de Route 53, los aceleradores estándar de Global Accelerator y cualquier equilibrador de carga de aplicaciones con Shield

Advanced. Al proteger los balanceadores de carga de aplicaciones, puede asociar las ACL AWS WAF web y crear reglas basadas en la velocidad para ellas. Puede configurar la interacción proactiva con el SRT tanto para sus aceleradores estándar de Global Accelerator como para sus equilibradores de carga de aplicaciones asociando comprobaciones de estado de Route 53 nuevas o existentes. Para obtener más información sobre las opciones, consulte Protecciones de recursos en AWS Shield Advanced.

El siguiente diagrama de referencia muestra un ejemplo de arquitectura resistente a los ataques DDoS para aplicaciones TCP y UDP.



Los beneficios que este enfoque proporciona a su aplicación incluyen los siguientes:

- Protección contra los ataques DDoS más grandes conocidos en la capa de infraestructura (capa 3 y capa 4). Si el volumen de un ataque provoca congestión desde el principio AWS, la falla se aislará más cerca de su origen y tendrá un efecto mínimo en los usuarios legítimos.
- Protección contra los ataques a la capa de aplicaciones del DNS, ya que Route 53 es responsable de ofrecer respuestas de DNS fiables.

- Si tiene una aplicación web, este enfoque proporciona protección contra las inundaciones de solicitudes en la capa de aplicaciones web. La regla basada en la velocidad que configuras en tu ACL AWS WAF web bloquea las IP de origen mientras envían más solicitudes de las que permite la regla.
- Interacción proactiva con el equipo de respuesta de Shield (SRT), si decide habilitar esta opción para los recursos elegibles. Cuando Shield Advanced detecta un evento que afecta al estado de su aplicación, el SRT responde e interactúa de forma proactiva con sus equipos de seguridad u operaciones utilizando la información de contacto que proporcione.

Ejemplos de casos de uso de Shield Advanced

Puede utilizar Shield Advanced para proteger sus recursos en muchos tipos de situaciones. Sin embargo, en algunos casos, debe utilizar otros servicios o combinar otros servicios con Shield Advanced para ofrecer la mejor protección. Los siguientes son ejemplos de cómo usar Shield Advanced u otros AWS servicios para ayudar a proteger sus recursos.

Objetivo	Servicios sugeridos	Documentación del servicio relacionada
Proteger una aplicación web y las API RESTful frente a ataques DDoS	Shield Advanced protege una CloudFront distribución de Amazon y un Application Load Balancer	Documentación de Elastic Load Balancing, CloudFront documentación de Amazon
Proteger una aplicación basada en TCP frente a un ataque DDoS	Shield Advanced protege un acelerador AWS Global Accelerator estándar; se adjunta a una dirección IP elástica	AWS Global Accelerator Documentación, documentación de Elastic Load Balancing
Proteger un servidor de juegos basado en UDP frente a un ataque DDoS	Shield Advanced protege una instancia de Amazon EC2 asociada a una dirección IP elástica	Documentación de Amazon Elastic Compute Cloud

Por ejemplo, si usa Shield Advanced para proteger una dirección IP elástica, Shield Advanced protege cualquier recurso que esté asociado a ella. Durante un ataque, Shield Advanced despliega automáticamente las ACL de la red en el borde de la AWS red. Cuando las ACL de red están en el borde de la red, Shield Advanced puede proporcionar protección contra eventos de DDoS más grandes. Normalmente, las ACL de red se aplican cerca de sus instancias de Amazon EC2 dentro de su Amazon VPC. La ACL de red puede mitigar ataques tan grandes como el volumen que puedan gestionar la instancia y Amazon VPC. Por ejemplo, si la interfaz de red asociada a la instancia de Amazon EC2 puede procesar hasta 10 Gbps, los volúmenes superiores a 10 Gbps ralentizarán y, posiblemente, bloquearán el tráfico a dicha instancia. Durante un ataque, Shield Advanced promueve la ACL de red a la frontera de AWS , lo que permite procesar varios terabytes de tráfico. Su ACL de red puede proporcionar protección a sus recursos más allá de la capacidad normal de su red. Para obtener más información acerca de las ACL de red, consulte ACL de red.

Empezar con AWS Shield Advanced

En este tutorial se explica cómo empezar a AWS Shield Advanced utilizar la consola Shield Advanced.

> **Note**
>
> Shield Advanced requiere una suscripción, pero AWS Shield Standard no la necesita. Las protecciones proporcionadas por Shield Standard están disponibles de forma gratuita para todos los clientes de AWS .

Shield Advanced proporciona detección y protección de mitigación de DDoS avanzadas contra los ataques a la capa de red (capa 3), la capa de transporte (capa 4) y la capa de aplicación (capa 7). Para obtener más información sobre Shield Advanced, consulte AWS Shield Advanced visión general.

La comunidad AWS técnica ha publicado un ejemplo de un proceso automatizado para configurar Shield Advanced utilizando las herramientas de infraestructura como código (IaC) AWS CloudFormation y Terraform. Puede utilizarla AWS Firewall Manager con esta solución si sus cuentas forman parte de una organización AWS Organizations y si está protegiendo algún tipo de recurso, excepto Amazon Route 53 o AWS Global Accelerator. Para explorar esta opción, consulte el repositorio de código en aws-samples/ aws-shield-advanced-one-click-deployment y el tutorial en One-click deployment of Shield Advanced.

> **Note**
>
> Es importante que configure completamente Shield Advanced antes de que se produzca un evento de denegación de servicio distribuido (DDoS). Complete la configuración para garantizar que su aplicación esté protegida y que se ha preparado para responder en caso de que su aplicación se vea afectada por un ataque DDoS.

Realice los siguientes pasos en secuencia para empezar a utilizar Shield Advanced.

Contenido

Suscríbase a AWS Shield Advanced

Debe suscribirse a Shield Advanced para cada uno de los productos Cuenta de AWS que desee proteger. No es necesario suscribirse a Shield Standard.

Facturación de suscripciones de Shield Advanced

Si es distribuidor de AWS canales, póngase en contacto con su equipo de cuentas para obtener información y orientación. Esta información de facturación es para clientes que no son distribuidores de AWS canal.

Para todos los demás, se aplican las siguientes pautas de suscripción y facturación:

- En el caso de las cuentas que son miembros de una AWS Organizations organización, AWS factura las suscripciones de Shield Advanced a la cuenta de pagador de la organización, independientemente de si la propia cuenta de pagador está suscrita.

- Al suscribir varias cuentas que pertenezcan a la misma familia de cuentas de facturación de AWS Organizations consolidada, un único precio de suscripción cubre todas las cuentas suscritas de la familia. La organización debe ser propietaria de todas las Cuentas de AWS y de todos sus recursos.
- Si suscribe varias cuentas para varias organizaciones, puede seguir pagando una única cuota de suscripción para todas las organizaciones, cuentas y recursos, siempre que sea el propietario de todos ellos. Póngase en contacto con su administrador de cuentas o con el servicio de AWS asistencia y solicite una exención de las tarifas de AWS Shield Advanced suscripción para todas las organizaciones excepto una.

Para obtener ejemplos e información detallada sobre precios, consulte Precios de AWS Shield.

Simplifica las suscripciones con AWS Firewall Manager

Si sus cuentas forman parte de una organización, le recomendamos que utilice AWS Firewall Manager si puede, para automatizar las suscripciones y las protecciones de la organización. Firewall Manager admite todos los tipos de recursos protegidos, excepto Amazon Route 53 y AWS Global Accelerator. Para usar Firewall Manager, consulte AWS Firewall Manager y Cómo empezar con AWS Firewall ManagerAWS Shield Advanced las políticas.

Si no usa el Firewall Manager, suscríbase y agregue protecciones para cada cuenta con recursos que proteger mediante los siguientes procedimientos.

Para suscribirse a una cuenta a AWS Shield Advanced

1. Inicie sesión en la AWS Management Console consola AWS WAF & Shield y ábrala en https://console.aws.amazon.com/wafv2/.
2. En la barra de navegación de AWS Shield, seleccione Introducción. Seleccione Suscribirse a Shield Advanced.
3. En la página Suscribirse a Shield Advanced, lea cada término del acuerdo y, a continuación, marque todas las casillas de verificación para indicar que acepta los términos. En el caso de una familia de facturación consolidada, debe aceptar los términos de cada cuenta.

> **Important**
>
> Cuando esté suscrito, para cancelar la suscripción, debe ponerse en contacto con AWS Support.

Para deshabilitar la renovación automática de su suscripción, debe usar la operación Shield API o el comando de CLI UpdateSubscriptionupdate-subscription.

Seleccione Suscribirse a Shield Advanced. De este modo suscribe su cuenta a Shield Advanced y activa el servicio.

Su cuenta está suscrita. Siga estos pasos para proteger los recursos de su cuenta con Shield Advanced.

> **Note**
>
> Shield Advanced no protege automáticamente los recursos después de suscribirse. Debe especificar los recursos donde desea que Shield Advanced proteja y configure las protecciones.

Agregue recursos para proteger y configurar las protecciones

Shield Advanced solo protege los recursos que se especifiquen, ya sea mediante Shield Advanced o en una política Shield Advanced de Firewall Manager. No protege automáticamente los recursos de una cuenta suscrita.

Si utilizas una póliza AWS Firewall Manager Shield Advanced para tus protecciones, no necesitas realizar este paso. La política se configura con los tipos de recursos que se van a proteger y Firewall Manager agrega automáticamente protecciones a los recursos que se encuentren dentro del ámbito de la política.

Si no usa Firewall Manager, siga los siguientes procedimientos para toda cuenta donde tenga recursos que proteger.

Elección de los recursos que se van a proteger con Shield Advanced

1. Seleccione Agregar recursos que se protegerán en la página de confirmación de la suscripción del procedimiento anterior o en la página Recursos protegidos u Información general.
2. En la página Elegir los recursos que se protegerán con Shield Advanced, en Especificar la región y los tipos de recursos, proporcione las especificaciones de región y de tipo de recurso de los recursos que desea proteger. Puede proteger los recursos de varias regiones seleccionando

Todas las regiones y puede limitar la selección a los recursos globales seleccionando Global. Puede deseleccionar cualquier tipo de recurso que no desee proteger. Para obtener información sobre las protecciones de sus tipos de recursos, consulte AWS Shield Advanced protecciones por tipo de recurso.

3. Elija Cargar recursos. Shield Advanced rellena la sección Seleccionar recursos con los recursos de AWS que coinciden con sus criterios.
4. En la sección Seleccionar recursos, puede filtrar la lista de recursos introduciendo una cadena para buscarla en las listas de recursos.

   Seleccione los recursos que desea proteger.
5. En la sección Etiquetas, si desea agregar etiquetas a las protecciones Shield Advanced que está creando, especifíquelas. Para obtener información acerca de cómo etiquetar los recursos de AWS , consulte Uso de Tag Editor.
6. Elija Proteger con Shield Advanced. Esto agrega las protecciones de Shield Advanced a los recursos.

Continúe recorriendo las pantallas del asistente de la consola para completar la configuración de las protecciones de sus recursos.

Temas

- Configure las protecciones DDoS de la capa de aplicación (capa 7) con AWS WAF
- Configure una detección basada en el estado para sus protecciones
- Configuración de alarmas y notificaciones
- Revise y finalice la configuración de protección

Configure las protecciones DDoS de la capa de aplicación (capa 7) con AWS WAF

Para proteger un recurso de la capa de aplicación, Shield Advanced utiliza una ACL AWS WAF web con una regla basada en la velocidad como punto de partida. AWS WAF es un firewall de aplicaciones web que permite supervisar las solicitudes HTTP y HTTPS que se reenvían a los recursos de la capa de aplicaciones y controlar el acceso al contenido en función de las características de las solicitudes. Una regla basada en tasas limita el volumen de tráfico en función de los criterios de agregación de solicitudes, lo que proporciona una protección DDoS básica a la aplicación. Para más información, consulte Cómo AWS WAF funciona y Instrucción de regla basada en frecuencia.

También puede habilitar, de forma opcional, la mitigación automática de DDoS en la capa de aplicación de Shield Advanced, para limitar automáticamente las solicitudes de fuentes conocidas de DDoS y proporcionar protecciones específicas para cada incidente.

> **Important**
>
> Si administra sus protecciones de Shield Advanced AWS Firewall Manager mediante una política de Shield Advanced, no podrá administrar las protecciones de la capa de aplicación aquí. Debe administrarlas en su política de Shield Advanced de Firewall Manager.

Suscripciones y AWS WAF costos de Shield Advanced

Su suscripción a Shield Advanced cubre los costes de uso de AWS WAF las capacidades estándar para los recursos que proteja con Shield Advanced. Las AWS WAF tarifas estándar que cubren las protecciones Shield Advanced son el costo por ACL web, el costo por regla y el precio base por millón de solicitudes de inspección de solicitudes web, hasta 1500 WCU y hasta el tamaño de cuerpo predeterminado.

Al habilitar la mitigación automática de DDoS en la capa de aplicaciones de Shield Advanced, se añade un grupo de reglas a la ACL web que utiliza 150 unidades de capacidad (WCU) de ACL web. Estas WCU se tienen en cuenta para el uso de la WCU en su ACL web. Para obtener más información, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced, El grupo de reglas de Shield Advanced y AWS WAF unidades de capacidad ACL web (WCU).

Su suscripción a Shield Advanced no cubre el uso AWS WAF de recursos que no proteja con Shield Advanced. Tampoco cubre ningún AWS WAF coste adicional no estándar de los recursos protegidos. Algunos ejemplos de AWS WAF costes no estándar son los del control de bots, la acción de la CAPTCHA regla, las ACL web que utilizan más de 1500 WCU y la inspección del cuerpo de la solicitud por encima del tamaño predeterminado. La lista completa se encuentra en la página de precios. AWS WAF

Para obtener la información completa y ejemplos de precios, consulte Precios de Shield y Precios de AWS WAF.

Configuración de las protecciones DDoS de capa 7 para una región

Shield Advanced le ofrece la opción de configurar la mitigación de DDoS de capa 7 para cada región en la que se encuentren los recursos que elija. Si va a agregar protecciones en varias regiones, el asistente le guiará por el siguiente procedimiento para cada región.

1. La página Configurar las protecciones DDoS de capa 7 muestra todos los recursos que aun no están asociados a una ACL web. Para cada uno de ellos, elija una ACL web existente o cree una ACL web nueva. En el caso de cualquier recurso que ya tenga una ACL web asociada, puede cambiar las ACL web desasociando primero la actual mediante ella. AWS WAF Para obtener más información, consulte Asociar o desasociar una ACL web a un recurso AWS.

   En el caso de las ACL web que aun no tienen una regla basada en tasas, el asistente de configuración le pide que agregue una. Una regla basada en tasas limita el tráfico de las direcciones IP cuando estas envían un gran volumen de solicitudes. Las reglas basadas en tasas ayudan a proteger la aplicación frente a avalanchas de solicitudes web y pueden proporcionar alertas sobre picos repentinos de tráfico que pudieran indicar un posible ataque DDoS. Para agregar una regla basada en tasas a una ACL web, seleccione Agregar regla de límite de tasas y, a continuación, especifique una acción para limitar la tasa y establecer una regla. Puede configurar protecciones adicionales en la ACL web mediante. AWS WAF

   Para obtener información sobre el uso de las ACL web y las reglas basadas en tasas en sus protecciones de Shield Advanced, incluidas las opciones de configuración adicionales para las reglas basadas en tasas, consulte Shield: ACL AWS WAF web de capa de aplicación avanzada y reglas basadas en tasas.

2. Para la mitigación automática de DDoS en la capa de aplicación, si desea que Shield Advanced mitigue automáticamente los ataques DDoS contra los recursos de la capa de aplicaciones, elija Activar y, a continuación, seleccione la acción de AWS WAF regla que quiere que Shield Advanced utilice en sus reglas personalizadas. Esta configuración se aplica a todas las ACL web de los recursos que gestione en esta sesión del asistente.

   Con la mitigación automática de DDoS en la capa de aplicación, Shield Advanced mantiene una regla basada en la velocidad en la ACL AWS WAF web del recurso que limita el volumen de solicitudes de fuentes de DDoS conocidas. Además, Shield Advanced compara los patrones de tráfico actuales con las bases de referencia de tráfico históricas para detectar desviaciones que puedan indicar un ataque DDoS. Cuando Shield Advanced detecta un ataque DDoS, responde creando, evaluando e implementando AWS WAF reglas personalizadas para responder. Especifique si las reglas personalizadas cuentan o bloquean los ataques en su nombre.

   > **Note**
   >
   > La mitigación automática de DDoS a nivel de aplicación solo funciona con las ACL web que se crearon con la última versión de AWS WAF (v2).

Para obtener más información sobre la mitigación automática de DDoS en la capa de aplicaciones de Shield Advanced, incluidas las advertencias y las prácticas recomendadas para el uso de esta función, consulte. Mitigación de DDoS de la capa de aplicación automática de Shield Advanced

3. Elija Siguiente. El asistente de la consola pasa a la página de detección basada en el estado.

Configure una detección basada en el estado para sus protecciones

Configure Shield Advanced para utilizar la detección basada en el estado a fin de mejorar la capacidad de respuesta y la precisión en la detección y mitigación de ataques. Los controles de estado bien configurados son esenciales para una detección precisa de los eventos. Puede configurar la detección basada en el estado para cualquier tipo de recurso, excepto para las zonas alojadas en Route 53.

Para utilizar la detección basada en el estado, defina una comprobación de estado para su recurso en Route 53 y, a continuación, asocie la comprobación de estado a la protección Shield Advanced. Es importante que la comprobación de estado que configure refleje con precisión el estado del recurso. Para obtener información y ejemplos sobre cómo configurar las comprobaciones de estado para utilizarlas con Shield Advanced, consulte Detección basada en la salud mediante controles de salud.

Se requieren comprobaciones de estado para poder contar con el apoyo proactivo del equipo de respuesta de Shield (SRT). Para obtener información sobre la interacción proactiva, consulte Configuración de interacción proactiva.

> **Note**
>
> Las comprobaciones de estado deben declararse en buen estado cuando las asocie a sus protecciones de Shield Advanced.

Configuración de una detección basada en el estado

1. En Associated Health Check (Comprobación de estado asociada), elija el identificador de la comprobación de estado que desea asociar a la protección.

> **Note**
>
> Si no ve la comprobación de estado que necesita, vaya a la consola de Route 53 y verifique la comprobación de estado y su ID. Para obtener más información, consulte Creación y actualización de comprobaciones de estado.

2. Elija Siguiente. El asistente de la consola pasa a la página de alarmas y notificaciones.

Configuración de alarmas y notificaciones

Si lo desea, puede configurar las notificaciones de Amazon Simple Notification Service para las CloudWatch alarmas de Amazon detectadas y la actividad de las reglas basada en tasas. Puede utilizarlos para recibir notificaciones cuando Shield detecte un evento en un recurso protegido o cuando se supere un límite de tasa configurado en una regla basada en tasas.

Para obtener información sobre las CloudWatch métricas de Shield Advanced, consulteAWS Shield Advanced métricas. Para obtener información sobre Amazon SNS, consulte la Guía para desarrolladores de Amazon Simple Notification Service.

Configuración de alarmas y notificaciones

1. Seleccione los temas de Amazon SNS para los que desea recibir notificaciones. Puede usar un solo tema de Amazon SNS para todos los recursos protegidos y las reglas basadas en tasas, o puede elegir diferentes temas, personalizados para su organización. Por ejemplo, puede crear un tema de SNS para cada equipo responsable de la respuesta a incidentes para un conjunto específico de recursos.
2. Elija Siguiente. El asistente de la consola pasa a la página de revisión de la protección de recursos.

Revise y finalice la configuración de protección

Revisión y configuración de sus ajustes

1. En la página Revisar y configurar la visibilidad y la mitigación de los DDoS, revise sus ajustes. Para realizar modificaciones, elija Editar en el área que desee modificar. Esto lo lleva de vuelta a la página asociada del asistente de consola. Realice los cambios y, a continuación,

seleccione Siguiente en las páginas siguientes hasta que vuelva a la página Revisar y configurar la visibilidad y la mitigación de los DDoS.

2. Seleccione Finalizar la configuración. La página Recursos protegidos muestra los recursos recién protegidos.

Configurar el AWS soporte de SRT

El equipo de respuesta de Shield (SRT) está formado por ingenieros de seguridad que se especializan en la respuesta a eventos DDoS. Si lo desea, puede agregar permisos que permitan al SRT gestionar los recursos en su nombre durante un evento de DDoS. Además, puede configurar el SRT para que interactúe con usted de forma proactiva si las comprobaciones de estado de Route 53 asociadas a sus recursos protegidos no funcionan correctamente durante un evento detectado. Estas dos incorporaciones a sus protecciones permiten responder más rápidamente a los eventos de DDoS.

> **Note**
>
> Para utilizar los servicios del equipo de respuesta de Shield (SRT), debe haberse registrado en el plan de soporte Business o en el plan de soporte Enterprise.

El SRT puede monitorear los datos y registros de las AWS WAF solicitudes durante los eventos de la capa de aplicación para identificar el tráfico anómalo. Pueden ayudar a elaborar AWS WAF reglas personalizadas para mitigar las fuentes de tráfico infractoras. Según sea necesario, el SRT podría hacer recomendaciones de arquitectura para ayudarlo a alinear mejor sus recursos con AWS las recomendaciones.

Para obtener más información sobre la SRT, consulte Asistencia del equipo de respuesta de Shield (Shield Response Team, SRT).

Cómo conceder permisos al SRT

1. En la página de descripción general de la AWS Shield consola, en Configurar la compatibilidad con AWS SRT, selecciona Editar el acceso a SRT. Se abre la página de acceso al equipo de respuesta de Edit AWS Shield (SRT).
2. Para Configuración de acceso de SRT, seleccione una de las siguientes opciones:

- No conceder al SRT acceso a mi cuenta: Shield elimina cualquier permiso que se haya otorgado anteriormente al SRT para acceder a su cuenta y sus recursos.
- Crear un nuevo rol para que el SRT acceda a mi cuenta: Shield crea un rol que confía en la entidad principal del servicio `drt.shield.amazonaws.com`, que representa al SRT, y le asocia la política administrada `AWSShieldDRTAccessPolicy`. La política gestionada permite al SRT realizar AWS Shield Advanced llamadas a la AWS WAF API en tu nombre y acceder a tus AWS WAF registros. Para obtener más información sobre la política administrada, consulte AWS política gestionada: AWSShieldDRTAccessPolicy.
- Elija un rol existente para que el SRT pueda acceder a mis cuentas. Para elegir esta opción, debe modificar la configuración del rol en AWS Identity and Access Management (IAM) de la siguiente manera:
  - Asocie la política `AWSShieldDRTAccessPolicy` administrada al rol. Esta política gestionada permite al SRT realizar AWS Shield Advanced llamadas a la AWS WAF API en tu nombre y acceder a tus registros. AWS WAF Para obtener más información sobre la política administrada, consulte AWS política gestionada: AWSShieldDRTAccessPolicy. Para obtener información sobre cómo asociar la política administrada a su rol, consulte Asociar y desasociar políticas de IAM.
  - Modifique el rol para confiar en la entidad principal de servicio `drt.shield.amazonaws.com`. Esta es la entidad principal de servicio que representa el SRT. Para obtener más información, consulte Elemento de la política de JSON de IAM: Principal.

3. Elija Guardar para guardar los cambios.

Para obtener más información sobre cómo permitir que el SRT acceda a sus protecciones y datos, consulte Configuración del acceso para el equipo de respuesta de Shield (SRT).

Habilitación de la interacción proactiva de SRT

1. En la página de información general de la AWS Shield consola, en Interacción proactiva y contactos, en el área de contactos, selecciona Editar.

   En la página Editar contactos, proporcione la información de contacto de las personas con las que desea que el SRT se ponga en contacto para tener una interacción proactiva.

Si proporciona más de un contacto, en Notas, indique las circunstancias en las que debe utilizarse cada contacto. Incluya las designaciones de los contactos principales y secundarios y proporcione los horarios de disponibilidad y las zonas horarias de cada contacto.

Ejemplos de notas de contacto:

- Esta es una línea directa que cuenta con personal las 24 horas del día, todos los días de la semana, todos los días del año. Trabaje con el analista que le responda, le dirigirá a la persona adecuada en la llamada.
- Póngase en contacto conmigo si la línea directa no responde en 5 minutos.

2. Seleccione Save (Guardar).

   La página Información general refleja la información de contacto actualizada.

3. Seleccione Editar característica de interacción proactiva, seleccione Habilitar y, a continuación, seleccione Guardar para habilitar la interacción proactiva.

Para obtener más información sobre la interacción proactiva, consulte Configuración de interacción proactiva.

Cree un panel de control de DDoS CloudWatch y configure alarmas CloudWatch

Puedes monitorizar la posible actividad de DDoS con Amazon CloudWatch, que recopila datos sin procesar de Shield Advanced y los procesa para convertirlos en métricas legibles prácticamente en tiempo real. Puede utilizar las estadísticas CloudWatch para obtener una perspectiva del rendimiento de su aplicación o servicio web. Para obtener más información sobre el uso CloudWatch, consulta Qué hay CloudWatch en la Guía del CloudWatch usuario de Amazon.

- Para obtener instrucciones sobre cómo crear un CloudWatch panel de control, consulteMonitorización con Amazon CloudWatch.
- Para obtener descripciones de las métricas de Shield Advanced que puede agregar a su panel, consulte AWS Shield Advanced métricas.

Shield Advanced informa de las métricas de recursos con CloudWatch más frecuencia durante los eventos de DDoS que cuando no hay ningún evento en curso. Shield Advanced informa de las métricas una vez por minuto durante un evento y, después, una vez finalizado el evento. Aunque no

haya eventos en curso, Shield Advanced notifica las métricas una vez al día, a una hora asignada al recurso. Este informe periódico mantiene las métricas activas y disponibles para usarlas en sus CloudWatch alarmas personalizadas.

Con esto se completa el tutorial de introducción a Shield Advanced. Para aprovechar al máximo las protecciones que ha elegido, siga explorando las características y opciones de Shield Advanced. Para empezar, familiarícese con las opciones para ver y responder a los eventos en Visibilidad de los eventos de DDoS y Respuesta a eventos de DDoS.

Asistencia del equipo de respuesta de Shield (Shield Response Team, SRT)

El equipo de respuesta de Shield (SRT) proporciona asistencia adicional a los clientes de Shield Advanced. El SRT está formado por ingenieros de seguridad que se especializan en la respuesta a eventos DDoS. Como capa de apoyo adicional a su plan de AWS Support , puede trabajar directamente con el SRT y aprovechar su experiencia como parte de su flujo de trabajo de respuesta a eventos. Para obtener información acerca de las opciones y las instrucciones de configuración, consulte los siguientes temas.

> **Note**
>
> Para utilizar los servicios del equipo de respuesta de Shield (SRT), debe haberse registrado en el plan de soporte Business o en el plan de asistencia Enterprise.

Actividades de asistencia del SRT

El objetivo principal de una interacción con el SRT es proteger la disponibilidad y el rendimiento de su aplicación. Según el tipo de evento de DDoS y la arquitectura de la aplicación, el SRT puede llevar a cabo una o más de las siguientes acciones:

- AWS WAF análisis y reglas de registro: en el caso de los recursos que utilizan una ACL AWS WAF web, el SRT puede analizar sus AWS WAF registros para identificar las características de los ataques en las solicitudes web de su aplicación. Con su aprobación durante la interacción, el SRT puede aplicar cambios a su ACL web para bloquear los ataques que haya identificado.
- Crear mitigaciones de red personalizadas: el SRT puede crear mitigaciones personalizadas para los ataques a la capa de infraestructura. El SRT puede ayudarle a comprender el tráfico

esperado para su aplicación, bloquear el tráfico inesperado y optimizar los límites de velocidad de paquetes por segundo. Para obtener más información, consulte Configuración de mitigaciones personalizadas con el equipo de respuesta de Shield (SRT).

- Ingeniería de tráfico de red: el SRT trabaja en estrecha colaboración con los equipos de AWS redes para proteger a los clientes de Shield Advanced. Cuando sea necesario, AWS puede cambiar la forma en que el tráfico de Internet llega a la AWS red para asignar más capacidad de mitigación a su aplicación.
- Recomendaciones de arquitectura: el SRT puede determinar que la mejor mitigación de un ataque requiere cambios en la arquitectura para alinearlos mejor con las AWS mejores prácticas, y ayudarán a respaldar la implementación de estas prácticas. Para obtener información, consulte Prácticas recomendadas por AWS para la resiliencia ante los ataques DDoS.

Temas

Configuración del acceso para el equipo de respuesta de Shield (SRT)

Puedes conceder permiso al Shield Response Team (SRT) para que actúe en tu nombre, accediendo a tus AWS WAF registros y realizando llamadas a AWS WAF las API AWS Shield Advanced y a las API para gestionar las protecciones. Durante los eventos de DDoS en la capa de aplicación, el SRT puede supervisar AWS WAF las solicitudes para identificar el tráfico anómalo y ayudar a elaborar AWS WAF reglas personalizadas para mitigar las fuentes de tráfico infractoras.

Además, puede conceder al SRT acceso a otros datos que haya almacenado en los buckets de Amazon S3, como capturas de paquetes o registros de un Application Load Balancer, CloudFront Amazon o de fuentes de terceros.

> **Note**
>
> Para utilizar los servicios del equipo de respuesta de Shield (SRT), debe haberse registrado en el plan de soporte Business o en el plan de asistencia Enterprise.

Administración de los permisos del SRT

1. En la página de información general de la AWS Shield consola, en Configurar la compatibilidad con AWS SRT, selecciona Editar el acceso a SRT. Se abre la página de acceso al equipo de respuesta de Edit AWS Shield (SRT).
2. Para Configuración de acceso de SRT, seleccione una de las siguientes opciones:

   - No conceder al SRT acceso a mi cuenta: Shield elimina cualquier permiso que se haya otorgado anteriormente al SRT para acceder a su cuenta y sus recursos.
   - Crear un nuevo rol para que el SRT acceda a mi cuenta: Shield crea un rol que confía en la entidad principal del servicio `drt.shield.amazonaws.com`, que representa al SRT, y le asocia la política administrada `AWSShieldDRTAccessPolicy`. La política gestionada permite al SRT realizar AWS Shield Advanced llamadas a la AWS WAF API en tu nombre y acceder a tus AWS WAF registros. Para obtener más información sobre la política administrada, consulte AWS política gestionada: AWSShieldDRTAccessPolicy.
   - Elija un rol existente para que el SRT pueda acceder a mis cuentas. Para elegir esta opción, debe modificar la configuración del rol en AWS Identity and Access Management (IAM) de la siguiente manera:
     - Asocie la política `AWSShieldDRTAccessPolicy` administrada al rol. Esta política gestionada permite al SRT realizar AWS Shield Advanced llamadas a la AWS WAF API en tu nombre y acceder a tus registros. AWS WAF Para obtener más información sobre la política administrada, consulte AWS política gestionada: AWSShieldDRTAccessPolicy. Para obtener información sobre cómo asociar la política administrada a su rol, consulte Asociar y desasociar políticas de IAM.
     - Modifique el rol para confiar en la entidad principal de servicio `drt.shield.amazonaws.com`. Esta es la entidad principal de servicio que representa el SRT. Para obtener más información, consulte Elemento de la política de JSON de IAM: Principal.
3. Para (opcional): conceda acceso SRT a un bucket de Amazon S3. Si necesita compartir datos que no están en sus registros de ACL AWS WAF web, configúrelo. Por ejemplo, los registros de acceso de Application Load Balancer, los CloudFront registros de Amazon o los registros de fuentes de terceros.

> **Note**
>
> No necesitas hacer esto para tus registros de ACL AWS WAF web. El SRT obtiene acceso a ellos cuando conceda acceso a su cuenta.

a. Configure los buckets de Amazon S3 según las siguientes directrices:

   - Las ubicaciones de los cubos deben estar en las Cuenta de AWS mismas ubicaciones a las que le diste acceso general al SRT, en el paso anterior, el acceso al AWS Shield Response Team (SRT).
   - Los buckets pueden ser de texto sin formato o cifrado SSE-S3. Para obtener más información sobre el cifrado SSE-S3 de Amazon S3, consulte Protección de datos utilizando el cifrado del servidor con las claves de cifrado de Amazon S3-Managed Encryption Keys (SSE-S3) en la Guía del usuario de Amazon S3.

     El SRT no puede ver ni procesar los registros que están almacenados en depósitos cifrados con claves almacenadas en (). AWS Key Management Service AWS KMS

b. En la sección (Opcional): Conceder al SRT acceso a un bucket de Amazon S3, introduzca el nombre del bucket y elija Agregar bucket para cada bucket de Amazon S3 en el que se almacenen sus datos o registros. Puede agregar hasta 10 buckets.

   Esto otorga al SRT los siguientes permisos en cada bucket: `s3:GetBucketLocation`, `s3:GetObject` y `s3:ListBucket`.

   Si quiere dar permiso al SRT para acceder a más de 10 buckets, puede hacerlo editando las políticas de bucket adicionales y concediendo manualmente los permisos que se indican aquí para el SRT.

   A continuación, se muestra una lista de políticas de ejemplo.

```
{
    "Sid": "AWSDDoSResponseTeamAccessS3Bucket",
    "Effect": "Allow",
    "Principal": {
        "Service": "drt.shield.amazonaws.com"
    },
    "Action": [
```

```
            "s3:GetBucketLocation",
            "s3:GetObject",
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::bucket-name",
            "arn:aws:s3:::bucket-name/*"
        ]
}
```

4. Elija Guardar para guardar los cambios.

También puedes autorizar el SRT a través de la API creando un rol de IAM, adjuntándole la política y, a continuación, pasando el rol AWSShieldDRTAccessPolicy a la operación AssociatedRTrole.

Configuración de interacción proactiva

Con una interacción proactiva, el equipo de respuesta de Shield (SRT) se pone en contacto con usted directamente cuando la disponibilidad o el rendimiento de su aplicación se ve afectado por un posible ataque. Recomendamos este modelo de interacción porque proporciona la respuesta más rápida del SRT y le permite empezar a solucionar problemas incluso antes de ponerse en contacto con usted.

La participación proactiva está disponible para eventos de capa de red y capa de transporte en direcciones IP elásticas y aceleradores AWS Global Accelerator estándar, y para inundaciones de solicitudes web en CloudFront distribuciones de Amazon y balanceadores de carga de aplicaciones. La interacción proactiva solo está disponible para las protecciones de recursos de Shield Advanced que tengan una comprobación de estado de Amazon Route 53 asociada. Para obtener información acerca de la administración y el uso de las comprobaciones de estado, consulte Detección basada en la salud mediante controles de salud.

Durante un evento detectado por Shield Advanced, el SRT utiliza el estado de sus comprobaciones de estado para determinar si el evento cumple los requisitos para una interacción proactiva. En caso afirmativo, el SRT se pondrá en contacto con usted de acuerdo con las instrucciones de contacto que haya proporcionado en su configuración de interacción proactiva.

Puede configurar hasta diez contactos para una interacción proactiva y puede dar indicaciones que sirvan de guía al SRT para contactar con usted. Sus contactos de interacción proactiva deberían estar disponibles para interactuar con la SRT durante los eventos. Si no dispone de un centro de

operaciones abierto las 24 horas del día, los siete días de la semana, puede proporcionar un número de busca e indicar esta preferencia de contacto en sus indicaciones de contacto.

Para utilizar la interacción proactiva, debe hacer lo siguiente:

- Debe estar suscrito al plan Business Support o en el plan Enterprise Support.
- Debe asociar una comprobación de estado de Amazon Route 53 a cualquier recurso que desee proteger mediante la interacción proactiva. El SRT utiliza el estado de sus comprobaciones de estado para determinar si un evento requiere de una interacción proactiva, por lo que es importante que sus controles de estado reflejen con precisión el estado de sus recursos protegidos. Para obtener más información y orientación, consulte Detección basada en la salud mediante controles de salud.
- Para un recurso que tenga una ACL AWS WAF web asociada, debe crear la ACL web con AWS WAF (v2), que es la versión más reciente de. AWS WAF
- Debe proporcionar al menos un contacto para que el SRT lo utilice para la interacción proactiva durante un evento. Mantenga la información de contacto completa y actualizada.

Habilitación de la interacción proactiva de SRT

1. En la página de descripción general de la AWS Shield consola, en Participación proactiva y contactos, en el área de contactos, seleccione Editar.

   En la página Editar contactos, proporcione la información de contacto de las personas con las que desea que el SRT se ponga en contacto para tener una interacción proactiva.

   Si proporciona más de un contacto, en Notas, indique las circunstancias en las que debe utilizarse cada contacto. Incluya las designaciones de los contactos principales y secundarios y proporcione los horarios de disponibilidad y las zonas horarias de cada contacto.

   Ejemplos de notas de contacto:

   - Esta es una línea directa que cuenta con personal las 24 horas del día, todos los días de la semana, todos los días del año. Trabaje con el analista que le responda, le dirigirá a la persona adecuada en la llamada.
   - Póngase en contacto conmigo si la línea directa no responde en 5 minutos.
2. Seleccione Save (Guardar).

   La página Información general refleja la información de contacto actualizada.

3. Seleccione Editar característica de interacción proactiva, seleccione Habilitar y, a continuación, seleccione Guardar para habilitar la interacción proactiva.

Contactar con el equipo de respuesta de Shield (SRT)

Puede ponerse en contacto con el equipo de respuesta de Shield (SRT) de una de las siguientes maneras:

Caso de soporte

Puede abrir un caso en AWS Shield a través de la consola del Centro de Soporte de AWS .

Para obtener información sobre cómo crear un caso de soporte, consulte el Centro de AWS Support.

Seleccione la gravedad de su situación y proporcione sus datos de contacto. En la descripción, proporcione tantos detalles como sea posible. Facilite información sobre los recursos protegidos que crea que pueden verse afectados y el estado actual de su experiencia de usuario final. Por ejemplo, si su experiencia de usuario está degradada o hay partes de la aplicación que no están disponibles actualmente, proporcione esa información.

- En caso de sospecha de ataques DDoS: Si la disponibilidad o el rendimiento de su aplicación se están viendo afectados por un posible ataque DDoS, elija la gravedad y las siguientes opciones de contacto:
  - En cuanto a la gravedad, elija la gravedad más alta disponible para su plan de asistencia:
    - Para la asistencia Business, es Sistema de producción caído: < 1 hora.
    - Para la asistencia Enterprise, es Sistema esencial para la empresa caído: < 15 minutos.
  - Para la opción de contacto, seleccione Teléfono o Chat y facilite sus datos. El uso de un método de contacto en directo ofrece la respuesta más rápida.

Interacción proactiva

Con una participación AWS Shield Advanced proactiva, el SRT se pone en contacto con usted directamente si la comprobación de estado de Amazon Route 53 asociada a su recurso protegido deja de funcionar durante un evento detectado. Para obtener más información acerca de esta opción, consulte Configuración de interacción proactiva.

Configuración de mitigaciones personalizadas con el equipo de respuesta de Shield (SRT)

Para sus IP elásticas (eIP) y sus aceleradores AWS Global Accelerator estándar, puede trabajar con el equipo de respuesta de Shield (SRT) para configurar mitigaciones personalizadas. Esto resulta útil si conoce una lógica específica que deba aplicarse cuando se aplique una mitigación. Por ejemplo, es posible que desee permitir únicamente el tráfico procedente de determinados países, aplicar límites de tasa específicos, configurar validaciones opcionales, impedir los fragmentos o permitir únicamente el tráfico que coincida con un patrón específico en la carga útil del paquete.

A continuación, se muestran ejemplos de mitigaciones personalizadas comunes:

- Coincidencia de patrones: si opera un servicio que interactúa con aplicaciones del cliente, puede optar por hacer coincidir los patrones conocidos que sean exclusivos de esas aplicaciones. Por ejemplo, puede operar un servicio de juegos o comunicaciones que requiera que el usuario final instale el software específico que distribuye. Puede incluir un número mágico en cada paquete que la aplicación envíe a su servicio. Puede hacer coincidir hasta 128 bytes (separados o contiguos) de la carga útil y los encabezados de un paquete TCP o UDP no fragmentado. La coincidencia se puede expresar en notación hexadecimal como un desplazamiento específico desde el principio de la carga útil del paquete o un desplazamiento dinámico que sigue un valor conocido. Por ejemplo, la mitigación puede buscar el byte `0x01` y esperar que `0x12345678` sean los cuatro bytes siguientes.
- Específico del DNS: si utiliza su propio servicio de DNS autorizado mediante servicios como Global Accelerator o Amazon Elastic Compute Cloud (Amazon EC2), puede solicitar una mitigación personalizada que valide los paquetes para garantizar que son consultas de DNS válidas y aplicar una puntuación de sospecha que evalúe los atributos que sean específicos del tráfico de DNS.

Para obtener información sobre cómo trabajar con el SRT para crear mitigaciones personalizadas, cree un caso de asistencia en AWS Shield. Para obtener más información sobre la creación de AWS Support casos, consulte Cómo empezar con. AWS Support

Protecciones de recursos en AWS Shield Advanced

Puede añadir y configurar AWS Shield Advanced protecciones para sus recursos. Puede administrar las protecciones de un solo recurso y agrupar los recursos protegidos en colecciones lógicas para una mejor administración de los eventos. También puede realizar un seguimiento de los cambios en sus protecciones Shield Advanced utilizando AWS Config.

Temas

AWS Shield Advanced protecciones por tipo de recurso

Shield Advanced protege AWS los recursos en las capas de red y transporte (capas 3 y 4) y en la capa de aplicación (capa 7). Puede proteger algunos recursos directamente y otros asociándolos a recursos protegidos. Shield Advanced es compatible con IPv4 y no con IPv6.

En esta sección, se proporciona información sobre las protecciones de Shield Advanced para cada tipo de recurso.

> **Note**
>
> Shield Advanced protege solo los recursos que haya especificado en Shield Advanced o mediante una política avanzada de Shield Advanced de AWS Firewall Manager . No protege automáticamente sus recursos.

Puede usar Shield Advanced para una supervisión y protección avanzadas con los siguientes tipos de recursos:

- CloudFront Distribuciones de Amazon. Para CloudFront un despliegue continuo, Shield Advanced protege cualquier distribución provisional que esté asociada a una distribución principal protegida.
- Zonas alojadas de Amazon Route 53.
- AWS Global Accelerator aceleradores estándar.
- Direcciones IP elásticas de Amazon EC2. Shield Advanced protege los recursos asociados a las direcciones IP elásticas protegidas.
- Instancias de Amazon EC2, mediante la asociación a direcciones IP elásticas de Amazon EC2.
- Los siguientes equilibradores de carga Elastic Load Balancing (ELB):

- Equilibradores de carga de aplicación.
- Equilibradores de carga clásicos.
- Equilibradores de carga de red, mediante asociaciones a direcciones IP elásticas de Amazon EC2.

No puede usar Shield Advanced para proteger ningún otro tipo de recurso. Por ejemplo, no puede proteger los aceleradores de enrutamiento personalizados de AWS Global Accelerator ni los equilibradores de carga de puerta de enlace.

Puede supervisar y proteger hasta un máximo de 1000 recursos de cada uno de estos tipos de recursos por cuenta de Cuenta de AWS. Por ejemplo, en una sola cuenta, podría proteger 1000 direcciones IP elásticas de Amazon EC2, 1000 CloudFront distribuciones y 1000 balanceadores de carga de aplicaciones. Puede solicitar un aumento del número de recursos que puede proteger con Shield Advanced a través de la consola Service Quotas en https://console.aws.amazon.com/servicequotas/.

Protección de las instancias Amazon EC2 y los equilibradores de carga de red con Shield Advanced

Puede proteger las instancias Amazon EC2 y los equilibradores de carga de red adjuntando primero estos recursos a las direcciones IP elásticas y, a continuación, protegiendo las direcciones IP elásticas en Shield Advanced.

Al proteger las direcciones IP elásticas, Shield Advanced identifica y protege los recursos a los que están conectadas. Shield Advanced identifica automáticamente el tipo de recurso que está adjunto a una dirección IP elástica y aplica las detecciones y mitigaciones adecuadas para ese recurso. Esto incluye la configuración de ACL de red que son específicas de la dirección IP elástica. Para obtener más información sobre el uso de direcciones IP elásticas con sus recursos de AWS , consulte la siguiente guía: Documentación de Amazon Elastic Compute Cloud o Documentación del Equilibrador de carga elástico.

Durante un ataque, Shield Advanced despliega automáticamente las ACL de la red en el borde de la AWS red. Cuando las ACL de red están en el borde de la red, Shield Advanced puede proporcionar protección contra eventos de DDoS más grandes. Normalmente, las ACL de red se aplican cerca de sus instancias de Amazon EC2 dentro de su Amazon VPC. La ACL de red puede mitigar ataques tan grandes como el volumen que puedan gestionar la instancia y Amazon VPC. Por ejemplo, si la interfaz de red conectada a su instancia Amazon EC2 puede procesar hasta 10 Gbps, los volúmenes superiores a 10 Gbps se ralentizarán y posiblemente bloquearán el tráfico hacia esa instancia. Durante un ataque, Shield Advanced promueve la ACL de red a la frontera de AWS , lo que permite

procesar varios terabytes de tráfico. Su ACL de red puede proporcionar protección a sus recursos más allá de la capacidad normal de su red. Para obtener más información acerca de las ACL de red, consulte ACL de red.

Algunas herramientas de escalado AWS Elastic Beanstalk, por ejemplo, no permiten adjuntar automáticamente una dirección IP elástica a un Network Load Balancer. En esos casos, debe adjuntar manualmente la dirección IP elástica.

AWS Shield Advanced protecciones de capa de aplicación (capa 7)

Para proteger los recursos de la capa de aplicación con Shield Advanced, comience por asociar una ACL web de AWS WAF al recurso y agregarle una o más reglas basadas en tasas. Además, puede habilitar la mitigación automática de DDoS en la capa de aplicación, lo que hace que Shield Advanced cree y administre automáticamente reglas de ACL web en su nombre en respuesta a ataques DDoS.

Al proteger un recurso de la capa de aplicación con Shield Advanced, Shield Advanced analiza el tráfico a lo largo del tiempo para establecer y mantener las líneas base. Shield Advanced utiliza estas líneas base para detectar anomalías en los patrones de tráfico que podrían indicar un ataque DDoS. El punto en el que Shield Advanced detecta un ataque depende del tráfico que Shield Advanced haya podido observar antes del ataque y de la arquitectura que utilice para sus aplicaciones web. Las variaciones de arquitectura que pueden afectar al comportamiento de Shield Advanced incluyen el tipo de instancia que utilice, el tamaño de la instancia y si el tipo de instancia admite redes mejoradas. También puede configurar Shield Advanced para que mitigue automáticamente los ataques a la capa de aplicación.

Suscripciones y AWS WAF costos de Shield Advanced

Su suscripción a Shield Advanced cubre los costes de uso de AWS WAF las capacidades estándar para los recursos que proteja con Shield Advanced. Las AWS WAF tarifas estándar que cubren las protecciones Shield Advanced son el costo por ACL web, el costo por regla y el precio base por millón de solicitudes de inspección de solicitudes web, hasta 1500 WCU y hasta el tamaño de cuerpo predeterminado.

Al habilitar la mitigación automática de DDoS en la capa de aplicaciones de Shield Advanced, se añade un grupo de reglas a la ACL web que utiliza 150 unidades de capacidad (WCU) de ACL web. Estas WCU se tienen en cuenta para el uso de la WCU en su ACL web. Para obtener más información, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced, El grupo de reglas de Shield Advanced y AWS WAF unidades de capacidad ACL web (WCU).

Su suscripción a Shield Advanced no cubre el uso AWS WAF de recursos que no proteja con Shield Advanced. Tampoco cubre ningún AWS WAF coste adicional no estándar de los recursos protegidos. Algunos ejemplos de AWS WAF costes no estándar son los del control de bots, la acción de la CAPTCHA regla, las ACL web que utilizan más de 1500 WCU y la inspección del cuerpo de la solicitud por encima del tamaño predeterminado. La lista completa se encuentra en la página de precios. AWS WAF

Para obtener la información completa y ejemplos de precios, consulte Precios de Shield y Precios de AWS WAF.

Temas

- Detección y mitigación
- Shield: ACL AWS WAF web de capa de aplicación avanzada y reglas basadas en tasas
- Mitigación de DDoS de la capa de aplicación automática de Shield Advanced

Detección y mitigación

En esta sección se describen los factores que afectan a la detección y mitigación de los eventos de la capa de aplicación por parte de Shield Advanced.

Comprobaciones de estado

Los controles de estado que informan con precisión del estado general de su aplicación proporcionan a Shield Advanced información sobre las condiciones de tráfico que experimenta su aplicación. Shield Advanced requiere menos información que indique un posible ataque cuando la aplicación informa que está en mal estado y requiere más pruebas de un ataque si la aplicación informa que está en buen estado.

Es importante configurar los controles de estado para que informen con precisión del estado de la aplicación. Para obtener más información y orientación, consulte Detección basada en la salud mediante controles de salud.

Líneas base de tráfico

Las líneas base de tráfico proporcionan a Shield Advanced información sobre las características del tráfico normal de su aplicación. Shield Advanced utiliza estas líneas base para reconocer cuándo su aplicación no recibe tráfico normal, de modo que pueda notificárselo y, según esté configurado, empezar a diseñar y probar opciones de mitigación para contrarrestar un posible ataque. Para obtener información adicional sobre cómo Shield Advanced utiliza las líneas base de tráfico para

detectar posibles eventos, consulte la sección de información general. Lógica de detección de amenazas en la capa de aplicación

Shield Advanced crea sus líneas base a partir de la información proporcionada por la ACL web asociada al recurso protegido. La ACL web debe estar asociada al recurso durante al menos 24 horas y hasta 30 días antes de que Shield Advanced pueda determinar de forma fiable las líneas base de la aplicación. El tiempo necesario comienza cuando se asocia la ACL web, ya sea a través de Shield Advanced o a través de AWS WAF.

Para obtener más información sobre el uso de una ACL web con las protecciones de la capa de aplicación Shield Advanced, consulteShield: ACL AWS WAF web de capa de aplicación avanzada y reglas basadas en tasas.

Reglas basadas en frecuencia

Las reglas basadas en tasas pueden ayudar a mitigar los ataques. También pueden ocultar los ataques, mitigándolos antes de que se conviertan en un problema lo suficientemente grande como para que aparezcan en las líneas de referencia de tráfico normales o en los informes de estado de los controles de estado.

Le recomendamos que utilice reglas basadas en tasas en su ACL web cuando proteja un recurso de aplicación con Shield Advanced. Si bien sus medidas de mitigación pueden ocultar un posible ataque, son una valiosa primera línea de defensa, ya que ayudan a garantizar que su aplicación permanezca disponible para sus clientes legítimos. El tráfico que tus reglas basadas en tarifas detectan y el límite de velocidad se muestran en tus métricas. AWS WAF

Además de sus propias reglas basadas en tasas, si habilita la mitigación automática de DDoS en la capa de aplicación, Shield Advanced añade un grupo de reglas a su ACL web que utiliza para mitigar los ataques. En este grupo de reglas, Shield Advanced siempre cuenta con una regla basada en la velocidad que limita el volumen de solicitudes de direcciones IP que se sabe que son fuentes de ataques DDoS. Las métricas del tráfico que mitigan las reglas de Shield Advanced no están disponibles para que las veas.

Para obtener más información sobre las reglas basadas en tarifas, consulteInstrucción de regla basada en frecuencia. Para obtener información sobre la regla basada en tasas que Shield Advanced utiliza para la mitigación automática de DDoS en la capa de aplicación, consulte. El grupo de reglas de Shield Advanced

Para obtener más información sobre Shield Advanced y AWS WAF las métricas, consulteMonitorización con Amazon CloudWatch.

Shield: ACL AWS WAF web de capa de aplicación avanzada y reglas basadas en tasas

Para proteger un recurso de la capa de aplicación con Shield Advanced, comience por asociar una ACL AWS WAF web al recurso. AWS WAF es un firewall de aplicaciones web que permite supervisar las solicitudes HTTP y HTTPS que se reenvían a los recursos de la capa de aplicaciones y controlar el acceso al contenido en función de las características de las solicitudes. Puede configurar una ACL web para supervisar y administrar las solicitudes en función de factores como el origen de la solicitud, el contenido de las cadenas de consulta y las cookies, y la tasa de solicitudes procedentes de una sola dirección IP. Como mínimo, su protección Shield Advanced requiere que asocie una ACL web a una regla basada en tasas, que limita la tasa de solicitudes para cada dirección IP.

Si la ACL web asociada no tiene definida una regla basada en tasas, Shield Advanced le pide que defina al menos una. Las reglas basadas en tasas bloquean automáticamente el tráfico de las IP de origen cuando superan los umbrales que defina. Ayudan a proteger la aplicación frente a avalanchas de solicitudes web y pueden proporcionar alertas sobre picos repentinos de tráfico que pudieran indicar un posible ataque DDoS.

> **Note**
>
> Una regla basada en la velocidad responde muy rápidamente a los picos de tráfico que la regla supervisa. Por ello, una regla basada en la velocidad puede impedir no solo un ataque, sino también la detección de un posible ataque mediante la detección de Shield Advanced. Esta compensación favorece la prevención por encima de la visibilidad total de los patrones de ataque. Te recomendamos que utilices una regla basada en la velocidad como primera línea de defensa contra los ataques.

Una vez establecida la ACL web, si se produce un ataque DDoS, se aplican medidas de mitigación mediante la adición y la gestión de reglas en la ACL web. Puede hacerlo directamente, con la ayuda del equipo de respuesta de Shield (SRT) o automáticamente mediante la mitigación automática de DDoS en la capa de aplicación.

> **Important**
>
> Si también utiliza la mitigación automática de DDoS en la capa de aplicación, consulte las prácticas recomendadas para gestionar su ACL web en. Prácticas recomendadas para utilizar la mitigación automática

Comportamiento predeterminado de las reglas basado en la velocidad

Cuando utiliza una regla basada en tasas con su configuración predeterminada, evalúa AWS WAF periódicamente el tráfico durante el intervalo de tiempo anterior de 5 minutos. AWS WAF bloquea las solicitudes de cualquier dirección IP que supere el umbral de la regla hasta que la tasa de solicitudes baje a un nivel aceptable. Al configurar una regla basada en la velocidad a través de Shield Advanced, configure su umbral de velocidad en un valor superior a la velocidad de tráfico normal que espera de cualquier IP de origen en cualquier intervalo de tiempo de cinco minutos.

Es posible que desee utilizar más de una regla basada en tasas en una ACL web. Por ejemplo, podría tener una regla basada en tasas con un umbral alto para todo el tráfico, además de una o más reglas adicionales configuradas para que coincidan con determinadas partes de la aplicación web y que tengan umbrales más bajos. Por ejemplo, puede hacer coincidir el URI `/login.html` con un umbral más bajo para evitar abusos en una página de inicio de sesión.

Puede configurar una regla basada en la tasa para utilizar un intervalo de tiempo de evaluación diferente y para agregar las solicitudes en función de varios componentes de la solicitud, como los valores de los encabezados, las etiquetas y los argumentos de consulta. Para obtener más información, consulte Instrucción de regla basada en frecuencia.

Para obtener información y orientación adicionales, consulte la entrada del blog sobre seguridad Las tres reglas AWS WAF basadas en tarifas más importantes.

Se ampliaron las opciones de configuración mediante AWS WAF

La consola Shield Advanced le permite añadir una regla basada en tasas y configurarla con los ajustes básicos predeterminados. Puede definir opciones de configuración adicionales gestionando sus reglas basadas en tarifas mediante. AWS WAF Por ejemplo, puede configurar la regla para agregar las solicitudes en función de claves como una dirección IP reenviada, una cadena de consulta y una etiqueta. También puede añadir una declaración de restricción a la regla para filtrar algunas solicitudes de evaluación y limitación de tasas. Para obtener más información, consulte Instrucción de regla basada en frecuencia. Para obtener información sobre cómo AWS WAF

administrar las reglas de supervisión y administración de las solicitudes web, consulteCrear una ACL web.

Mitigación de DDoS de la capa de aplicación automática de Shield Advanced

Puede configurar Shield Advanced para que responda automáticamente y mitigue los ataques de capa de aplicación (capa 7) contra recursos protegidos de la capa de aplicaciones mediante el conteo o el bloqueo de las solicitudes web que formen parte del ataque. Esta opción es una adición a la protección de la capa de aplicación que se agrega a través de Shield Advanced con una ACL AWS WAF web y su propia regla basada en la tasa.

Cuando la mitigación automática está habilitada para un recurso, Shield Advanced mantiene un grupo de reglas en la ACL web asociada al recurso, donde administra las reglas de mitigación en su nombre. El grupo de reglas contiene una regla basada en tasas que rastrea el volumen de solicitudes de direcciones IP que se sabe que son fuentes de ataques DDoS.

Además, Shield Advanced compara los patrones de tráfico actuales con las bases de referencia de tráfico históricas para detectar desviaciones que puedan indicar un ataque DDoS. Shield Advanced responde a los ataques DDoS detectados mediante la creación, evaluación e implementación de AWS WAF reglas personalizadas adicionales en el grupo de reglas.

Contenido

- Cambio de la acción utilizada para la mitigación automática de DDoS en la capa de aplicación
- Se utiliza AWS CloudFormation con la mitigación automática de DDoS en la capa de aplicación

Advertencias sobre el uso de la mitigación automática

La siguiente lista describe las advertencias de la mitigación automática de DDoS en la capa de aplicación de Shield Advanced y describe los pasos que puede realizar en respuesta.

- La mitigación automática de DDoS en la capa de aplicación solo funciona con las ACL web que se crearon con la última versión de AWS WAF (v2).
- Shield Advanced necesita tiempo para establecer una línea base del tráfico normal e histórico de la aplicación, que aprovecha para detectar y aislar el tráfico de ataque del tráfico normal, a fin de mitigar el tráfico de ataques. El tiempo necesario para establecer una línea base es de 24 horas a 30 días a partir del momento en que se asocia una ACL web al recurso de aplicación protegido. Para obtener información adicional sobre las líneas base de tráfico, consulte. Detección y mitigación
- Al habilitar la mitigación automática de DDoS en la capa de aplicación, se agrega un grupo de reglas a la ACL web que utiliza 150 unidades de capacidad (WCU) de la ACL web. Estas WCU se tienen en cuenta para el uso de la WCU en su ACL web. Para obtener más información, consulte El grupo de reglas de Shield Advanced y AWS WAF unidades de capacidad ACL web (WCU).
- El grupo de reglas Shield Advanced genera AWS WAF métricas, pero no se pueden ver. Esto es igual que para cualquier otro grupo de reglas que utilice en su ACL web pero que no sea de su propiedad, como los grupos de reglas de reglas AWS administradas. Para obtener más información sobre AWS WAF las métricas, consulteAWS WAF métricas y dimensiones. Para obtener información sobre esta opción de protección Shield Advanced, consulteMitigación de DDoS de la capa de aplicación automática de Shield Advanced.
- En el caso de las ACL web que protegen varios recursos, la mitigación automática solo implementa mitigaciones personalizadas que no afectan negativamente a ninguno de los recursos protegidos.
- El tiempo que transcurre entre el inicio de un ataque DDoS y el momento en que Shield Advanced aplica las reglas de mitigación automática personalizadas varía según el evento. Algunos ataques DDoS pueden terminar antes de que se implementen las reglas personalizadas. Otros ataques pueden producirse cuando ya existe una mitigación y, por lo tanto, podrían mitigarse con esas reglas desde el inicio del evento. Además, las reglas basadas en la velocidad del grupo de reglas ACL web y Shield Advanced pueden mitigar el tráfico de ataques antes de que se detecte como un posible evento.

- En el caso de los balanceadores de carga de aplicaciones que reciben tráfico a través de una red de entrega de contenido (CDN), como Amazon CloudFront, se reducirán las capacidades de mitigación automática de la capa de aplicaciones de Shield Advanced para esos recursos del Application Load Balancer. Shield Advanced utiliza atributos de tráfico del cliente para identificar y aislar el tráfico de ataque del tráfico normal hacia su aplicación y es posible que las CDN no conserven ni reenvíen los atributos de tráfico del cliente originales. Si las usas CloudFront, te recomendamos habilitar la mitigación automática en la distribución. CloudFront
- La mitigación automática de DDoS en la capa de aplicación no interactúa con los grupos de protección. Puede habilitar la mitigación automática para los recursos que se encuentran en grupos de protección, pero Shield Advanced no aplica automáticamente mitigaciones de ataques en función de los hallazgos de los grupos de protección. Shield Advanced aplica mitigaciones de ataque automáticas a recursos individuales.

Prácticas recomendadas para utilizar la mitigación automática

Siga las instrucciones que se proporcionan en esta sección cuando utilice la mitigación automática.

Administración de protecciones generales

Siga estas pautas para planificar e implementar sus protecciones de mitigación automática.

- Administre todas sus protecciones de mitigación automática a través de Shield Advanced o, si las utiliza AWS Firewall Manager para administrar la configuración de mitigación automática de Shield Advanced, a través de Firewall Manager. No mezcle el uso de Shield Advanced y Firewall Manager para administrar estas protecciones.
- Administre recursos similares con las mismas ACL web y la misma configuración de protección, y administre recursos distintos con ACL web diferentes. Cuando Shield Advanced mitiga un ataque DDoS en un recurso protegido, define las reglas para la ACL web asociada al recurso y, a continuación, las compara con el tráfico de todos los recursos asociados a la ACL web. Shield Advanced solo aplicará las reglas si no afectan negativamente a ninguno de los recursos asociados. Para obtener más información, consulte Cómo administra Shield Advanced la mitigación automática.
- En el caso de los balanceadores de carga de aplicaciones que tienen todo su tráfico de Internet redirigido por proxy a través de una CloudFront distribución de Amazon, solo habilita la mitigación automática en la CloudFront distribución. La CloudFront distribución siempre tendrá la mayor cantidad de atributos de tráfico originales, que Shield Advanced aprovecha para mitigar los ataques.

Optimización de la detección y la mitigación

Siga estas pautas para optimizar las protecciones que la mitigación automática proporciona a los recursos protegidos. Para obtener una descripción general de la detección y mitigación de la capa de aplicación, consulteDetección y mitigación.

- Configure los controles de estado de sus recursos protegidos y utilícelos para habilitar la detección basada en el estado en sus protecciones Shield Advanced. Para obtener instrucciones, consulte Detección basada en la salud mediante controles de salud.
- Activa la mitigación automática en Count el modo hasta que Shield Advanced haya establecido una línea base para el tráfico normal e histórico. Shield Advanced necesita de 24 horas a 30 días para establecer una línea base.

  Para establecer una base de patrones de tráfico normales se requiere lo siguiente:

  - La asociación de una ACL web con el recurso protegido. Puede utilizarla AWS WAF directamente para asociar su ACL web o puede hacer que Shield Advanced la asocie cuando active la protección de la capa de aplicaciones de Shield Advanced y especifique la ACL web que desee utilizar.
  - Flujo de tráfico normal hacia su aplicación protegida. Si su aplicación no experimenta un tráfico normal, por ejemplo, antes de que se inicie o si no tiene tráfico de producción durante períodos prolongados, no se podrán recopilar los datos históricos.

Administración de ACL web

Siga estas pautas para administrar las ACL web que utiliza con la mitigación automática.

- Si necesita reemplazar la ACL web asociada al recurso protegido, realice los siguientes cambios en este orden:

  1. En Shield Advanced, desactiva la mitigación automática.
  2. En AWS WAF, desasocie la antigua ACL web y asocie la nueva ACL web.
  3. En Shield Advanced, habilita la mitigación automática.

  Shield Advanced no transfiere automáticamente la mitigación automática de la antigua ACL web a la nueva.
- No elimine ninguna regla de grupo de reglas de las ACL web cuyo nombre comience por `ShieldMitigationRuleGroup`. Si elimina este grupo de reglas, deshabilita las protecciones que proporciona la mitigación automática de Shield Advanced para cada recurso asociado a

la ACL web. Además, Shield Advanced puede tardar algún tiempo en recibir la notificación del cambio y actualizar su configuración. Durante este tiempo, las páginas de la consola de Shield Advanced proporcionarán información incorrecta.

Para obtener más información acerca de este grupo de reglas, consulte El grupo de reglas de Shield Advanced.

- No modifique el nombre de una regla del grupo de reglas que comience por `ShieldMitigationRuleGroup`. Si lo hace, puede interferir en las protecciones que proporciona la mitigación automática de Shield Advanced a través de la ACL web.
- Al crear reglas y grupos de reglas, no utilice nombres que comiencen por `ShieldMitigationRuleGroup`. Shield Advanced utiliza esta cadena para gestionar las mitigaciones automáticas.
- Al administrar sus reglas de ACL web, no asigne una configuración de prioridad de 10.000.000. Shield Advanced asigna esta configuración de prioridad a su regla del grupo de reglas de mitigación automática cuando la agrega.
- Mantenga la prioridad de la regla `ShieldMitigationRuleGroup` en relación con las demás reglas de su ACL web para que se ejecute cuando desee. Shield Advanced añade la regla del grupo de reglas a la ACL web con una prioridad de 10.000.000 para que se ejecute después de las demás reglas. Si usa el asistente de AWS WAF consola para administrar su ACL web, ajuste la configuración de prioridad según sea necesario después de agregar reglas a la ACL web.
- Si las utiliza AWS CloudFormation para administrar sus ACL web, no necesita administrar la `ShieldMitigationRuleGroup` regla del grupo de reglas. Siga las instrucciones de Se utiliza AWS CloudFormation con la mitigación automática de DDoS en la capa de aplicación.

Configuración necesaria para habilitar la mitigación automática

La mitigación automática de Shield Advanced se habilita como parte de las protecciones DDoS de la capa de aplicación para su recurso. Para obtener información sobre cómo hacer esto con la consola, consulte Configure las protecciones DDoS en la capa de aplicación.

La función de mitigación automática requiere que haga lo siguiente:

- Asociar una ACL web al recurso: esto se requiere para cualquier protección de la capa de aplicación de Shield Advanced. Puede utilizar la misma ACL web para varios recursos. Recomendamos hacer esto solo para los recursos que tienen un tráfico similar. Para obtener información sobre las ACL web, incluidos los requisitos para utilizarlas con varios recursos, consulte Cómo AWS WAF funciona.

- Habilitación y configuración de la mitigación automática de DDoS en la capa de aplicación de Shield Advanced: al habilitarla, especifique si desea que Shield Advanced bloquee o cuente automáticamente las solicitudes web que determine que forman parte de un ataque DDoS. Shield Advanced agrega un grupo de reglas a la ACL web asociada y lo usa para administrar su respuesta a los ataques DDoS al recurso de forma dinámica. Para obtener información sobre las opciones de acción de las reglas, consulte Acción de regla.
- (Opcional, pero recomendable) Añadir una regla basada en la tasas a la ACL web: de forma predeterminada, la regla basada en tasas proporciona a su recurso una protección básica contra los ataques DDoS al evitar que una dirección IP individual envíe demasiadas solicitudes en poco tiempo. Para obtener información sobre las reglas basadas en tasas, incluidas las opciones de agregación de solicitudes personalizadas y algunos ejemplos, consulte Instrucción de regla basada en frecuencia.

Cómo administra Shield Advanced la mitigación automática

Los temas de la sección describen cómo administra Shield Advanced los cambios de configuración para la mitigación automática de DDoS en la capa de aplicación y cómo gestiona los ataques DDoS cuando la mitigación automática está habilitada.

Temas

- Qué ocurre cuando se habilita la mitigación automática
- Cómo responde Shield Advanced a los ataques DDoS con la mitigación automática
- Cómo Shield Advanced administra la configuración de acciones de las reglas
- Cómo administra Shield Advanced las mitigaciones cuando un ataque remite
- Qué ocurre cuando se deshabilita la mitigación automática

Qué ocurre cuando se habilita la mitigación automática

Al habilitar la mitigación automática, Shield Advanced hace lo siguiente:

- Según sea necesario, agrega un grupo de reglas para el uso avanzado de Shield: si la ACL AWS WAF web que ha asociado al recurso aún no tiene una AWS WAF regla de grupo de reglas dedicada a la mitigación automática de DDoS en la capa de aplicación, Shield Advanced agrega una.

  El nombre del grupo de reglas comienza con `ShieldMitigationRuleGroup`. El grupo de reglas siempre contiene una regla basada en tasas denominada

`ShieldKnownOffenderIPRateBasedRule`, que limita el volumen de solicitudes de direcciones IP que se sabe que son fuentes de ataques DDoS. Para obtener información adicional sobre el grupo de reglas de Shield Advanced y la regla ACL web en la que se referencia, consulte El grupo de reglas de Shield Advanced.

- Comienza a responder a los ataques DDoS frente al recurso: Shield Advanced responde automáticamente a los ataques DDoS contra el recurso protegido. Además de la regla basada en la tasa, que siempre está presente, Shield Advanced usa su grupo de reglas para implementar AWS WAF reglas personalizadas para la mitigación de los ataques DDoS. Shield Advanced adapta estas reglas a su aplicación y a los ataques que sufre, y las comprueba con el tráfico histórico del recurso antes de implementarlas.

Shield Advanced utiliza una única regla del grupo de reglas en cualquier ACL web que utilice para la mitigación automática. Si Shield Advanced ya ha agregado el grupo de reglas para otro recurso protegido, no agrega un grupo de reglas adicional a la ACL web.

La mitigación automática de DDoS en la capa de aplicación depende de la presencia del grupo de reglas para mitigar los ataques. Si el grupo de reglas se elimina de la ACL AWS WAF web por cualquier motivo, la eliminación deshabilita la mitigación automática de todos los recursos asociados a la ACL web.

Cómo responde Shield Advanced a los ataques DDoS con la mitigación automática

Cuando tiene habilitada la mitigación automática en un recurso protegido, la regla basada en tasas `ShieldKnownOffenderIPRateBasedRule` en el grupo de reglas de Shield Advanced responde automáticamente a los volúmenes de tráfico elevados procedentes de fuentes de DDoS conocidas. Este límite de tasas se aplica de forma rápida y actúa como defensa de primera línea contra los ataques.

Cuando Shield Advanced detecta un ataque, hace lo siguiente:

1. Intenta identificar una firma de ataque que aísle el tráfico de ataque del tráfico normal que llega a su aplicación. El objetivo es crear reglas de mitigación de DDoS de alta calidad que, una vez implementadas, solo afecten al tráfico de ataques y no al tráfico normal de la aplicación.
2. Evalúa la firma del ataque identificada comparándola con los patrones de tráfico históricos del recurso que está siendo atacado, así como de cualquier otro recurso que esté asociado a la misma ACL web. Shield Advanced realiza esta acción antes de implementar cualquier regla en respuesta al evento.

Dependiendo de los resultados de la evaluación, Shield Advanced realiza una de las siguientes acciones:

- Si Shield Advanced determina que la firma del ataque aísla solo el tráfico implicado en el ataque DDoS, implementa la firma en las reglas de AWS WAF en el grupo de reglas de mitigación de Shield Advance en la ACL web. Shield Advanced proporciona a estas reglas la configuración de acción que haya configurado para la mitigación automática del recurso, ya sea Count o Block.
- De lo contrario, Shield Advanced no aplica ninguna mitigación.

Durante un ataque, Shield Advanced envía las mismas notificaciones y proporciona la misma información de eventos que las protecciones básicas de la capa de aplicación de Shield Advanced. Puede ver la información sobre los eventos y los ataques DDoS, así como sobre las mitigaciones de los ataques de Shield Advanced, en la consola de eventos de Shield Advanced. Para obtener más información, consulte Visibilidad de los eventos de DDoS.

Si ha configurado la mitigación automática para usar la acción de la regla de Block y las reglas de mitigación que Shield Advanced ha implementado dan falsos positivos, puede cambiar la acción de la regla a Count. Para obtener información acerca de cómo hacerlo, consulte Cambio de la acción utilizada para la mitigación automática de DDoS en la capa de aplicación.

Cómo Shield Advanced administra la configuración de acciones de las reglas

Puede configurar la acción de la regla para sus mitigaciones automáticas hacia Block o Count.

Al cambiar la configuración de la acción de la regla de mitigación automática de un recurso protegido, Shield Advanced actualiza la configuración de todas las reglas del recurso. Actualiza todas las reglas que estén actualmente en vigor para el recurso en el grupo de reglas de Shield Advanced y utiliza la nueva configuración de acciones cuando crea nuevas reglas.

Para los recursos que utilizan la misma ACL web, si especifica acciones diferentes, Shield Advanced utiliza la configuración de acciones Block para la regla basada en tasas `ShieldKnownOffenderIPRateBasedRule` del grupo de reglas. Shield Advanced crea y administra otras reglas del grupo de reglas en nombre de un recurso protegido específico y usa la configuración de acciones que especificó para el recurso. Todas las reglas del grupo de reglas de Shield Advanced de una ACL web se aplican al tráfico web de todos los recursos asociados.

Un cambio en la configuración de acción puede tardar unos segundos en propagarse. Durante este tiempo, es posible que vea la configuración anterior en algunos lugares donde se usa el grupo de reglas y la nueva en otros lugares.

Puede cambiar la configuración de las acciones de las reglas de la configuración de mitigación automática en la página de eventos de la consola y en la página de configuración de la capa de aplicación. Para obtener información sobre la página de eventos, consulte Respuesta a eventos de DDoS. Para obtener información sobre la página de configuración, consulte Configure las protecciones DDoS en la capa de aplicación.

Cómo administra Shield Advanced las mitigaciones cuando un ataque remite

Cuando Shield Advanced determina que las reglas de mitigación que se desplegaron para un ataque concreto ya no son necesarias, las elimina del grupo de reglas de mitigación de Shield Advanced.

La eliminación de las reglas de mitigación no coincidirá necesariamente con el final del ataque. Shield Advanced monitorea los patrones de ataque que detecta en sus recursos protegidos. Podría defenderse de forma proactiva contra la repetición de un ataque con una firma específica manteniendo en vigor las reglas que ha aplicado contra la primera incidencia de este ataque. Según sea necesario, Shield Advanced aumenta el período de tiempo durante el que mantiene las reglas en vigor. De esta forma, Shield Advanced podría mitigar los ataques repetidos con una firma específica antes de que afecten a los recursos protegidos.

Shield Advanced nunca elimina la regla basada en tasas `ShieldKnownOffenderIPRateBasedRule`, que limita el volumen de solicitudes de direcciones IP que se sabe que son fuentes de ataques DDoS.

Qué ocurre cuando se deshabilita la mitigación automática

Al deshabilitar la mitigación automática de un recurso, Shield Advanced hace lo siguiente:

- Deja de responder automáticamente a los ataques DDoS: Shield Advanced interrumpe sus actividades de respuesta automática para el recurso.
- Elimina las reglas innecesarias del grupo de reglas de Shield Advanced: si Shield Advanced mantiene alguna regla en su grupo de reglas administrado en nombre del recurso protegido, la elimina.
- Elimina el grupo de reglas de Shield Advanced, si ya no está en uso: si la ACL web que ha asociado al recurso no está asociada a ningún otro recurso que tenga habilitada la mitigación automática, Shield Advanced elimina su regla del grupo de reglas de la ACL web.

El grupo de reglas de Shield Advanced

Shield Advanced administra las actividades de mitigación automáticas mediante reglas de un grupo de reglas del que es propietario y que administra por usted. Shield Advanced hace referencia al grupo de reglas con una regla de la ACL web que ha asociado a su recurso protegido.

La regla del grupo de reglas de su ACL web

La regla de grupo de reglas de Shield Advanced de su ACL web presenta las siguientes propiedades:

- Nombre: `ShieldMitigationRuleGroup_`*`account-id`*`_`*`web-acl-id`*`_`*`unique-identifier`*
- Unidades de capacidad de ACL web (WCU): 150. Estas WCU se tienen en cuenta para el uso de la WCU en su ACL web.

Shield Advanced crea esta regla en la ACL web con una configuración de prioridad de 10 000 000, de modo que se ejecute después de las demás reglas y grupos de reglas de la ACL web. AWS WAF ejecuta las reglas en una ACL web desde la configuración de prioridad numérica más baja hacia arriba. Durante la administración de la ACL web, esta configuración de prioridad puede cambiar.

La función de mitigación automática no consume recursos de AWS WAF adicionales de su cuenta, además de las WCU que utiliza el grupo de reglas de su ACL web. Por ejemplo, el grupo de reglas de Shield Advanced no se cuenta como uno de los grupos de reglas de su cuenta. Para obtener información sobre los límites de las cuentas AWS WAF, consulteAWS WAF cuotas.

Reglas en el grupo de reglas

Dentro del grupo de reglas Shield Advanced al que se hace referencia, Shield Advanced mantiene una regla basada en tasas `ShieldKnownOffenderIPRateBasedRule`, que limita el volumen de solicitudes de direcciones IP que se sabe que son fuentes de ataques DDoS. Esta regla sirve como primera línea de defensa contra cualquier ataque, ya que siempre está presente en el grupo de reglas y no se basa en el análisis de los patrones de tráfico para contener los ataques. La acción de esta regla se establece en la acción que elija para las mitigaciones automáticas, al igual que las demás reglas del grupo de reglas. Para obtener información acerca de las reglas basadas en tasas, consulte Instrucción de regla basada en frecuencia.

> **Note**
>
> La regla basada en la tasa `ShieldKnownOffenderIPRateBasedRule` funciona independientemente de la detección de eventos de Shield Advanced. Si bien la mitigación

automática está habilitada, esta regla limita la frecuencia de las direcciones IP que se sabe que son fuentes de ataques DDoS. Para estas direcciones IP, la limitación de velocidad de la regla puede evitar los ataques y también evitar que los ataques aparezcan en la información de detección de Shield Advanced. Esta compensación favorece la prevención por encima de la visibilidad completa de los patrones de ataque.

Además de la regla permanente basada en tarifas descrita anteriormente, el grupo de reglas contiene todas las reglas que Shield Advanced utiliza actualmente para mitigar los ataques DDoS. Shield Advanced agrega, modifica y elimina estas reglas según sea necesario. Para obtener más información, consulte Cómo administra Shield Advanced la mitigación automática.

Métricas

El grupo de reglas genera AWS WAF métricas, pero dado que este grupo de reglas es propiedad de Shield Advanced, estas métricas no están disponibles para su visualización. Para obtener más información, consulte AWS WAF métricas y dimensiones.

Administración de la mitigación automática de DDoS en la capa de aplicación

Utilice las instrucciones de esta sección para administrar las configuraciones automáticas de mitigación de DDoS en la capa de aplicación. Para obtener información sobre cómo funciona la mitigación automática, consulte los temas anteriores.

> **Note**
>
> Siga las prácticas recomendadas que se describen enPrácticas recomendadas para utilizar la mitigación automática.

Temas

- Visualización de la configuración de mitigación automática de DDoS en la capa de aplicación de un recurso
- Cómo habilitar y deshabilitar la mitigación automática de DDoS en la capa de aplicación
- Cambio de la acción utilizada para la mitigación automática de DDoS en la capa de aplicación
- Se utiliza AWS CloudFormation con la mitigación automática de DDoS en la capa de aplicación

Visualización de la configuración de mitigación automática de DDoS en la capa de aplicación de un recurso

Puede ver la configuración de mitigación automática de DDoS en la capa de aplicación de un recurso en la página Recursos protegidos y en las páginas de protecciones individuales.

Cómo ver la configuración de mitigación automática de DDoS en la capa de aplicación

1. Inicie sesión en la AWS Management Console consola AWS WAF & Shield y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel AWS Shield de navegación, elija Recursos protegidos. En la lista de recursos protegidos, la columna Mitigación automática de DDoS en la capa de aplicación indica si la mitigación automática está habilitada y, si lo está, la acción que Shield Advanced realizará en sus mitigaciones.

   También puede seleccionar cualquier recurso de la capa de aplicación para ver la misma información que aparece en la página de protecciones del recurso.

Cómo habilitar y deshabilitar la mitigación automática de DDoS en la capa de aplicación

En el siguiente procedimiento, se muestra cómo habilitar o deshabilitar la respuesta automática de un recurso protegido.

Para habilitar o deshabilitar la mitigación automática de DDoS a nivel de aplicación para un único recurso

1. Inicie sesión en la AWS Management Console consola AWS WAF & Shield y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel AWS Shield de navegación, elija Recursos protegidos.
3. En la pestaña Protecciones, seleccione el recurso de capa de aplicación para el que desee habilitar la mitigación automática. Se abre la página de protecciones del recurso.
4. En la página de protecciones del recurso, elija Editar.
5. En la página Configurar la mitigación de DDoS en la capa 7 para los recursos globales: opcional, de la mitigación automática de DDoS en la capa de aplicación, elija la opción que desee utilizar para las mitigaciones automáticas. Las opciones de la consola son las siguientes:

   - Mantener la configuración actual: no se realizan cambios en la configuración de mitigación automática del recurso protegido.

- Habilitar: se habilita la mitigación automática para el recurso protegido. Al elegir esta opción, seleccione también la acción de regla que desee que utilicen las mitigaciones automáticas en las reglas de ACL web. Para obtener información sobre la configuración de las acciones de las reglas, consulte Acción de regla.

  Si tu recurso protegido aún no tiene un historial de tráfico normal de aplicaciones, activa la mitigación automática en el Count modo hasta que Shield Advanced pueda establecer una línea base. Shield Advanced comienza a recopilar información para su punto de referencia al asociar una ACL web a su recurso protegido, y establecer un buen punto de referencia del tráfico normal puede tardar de 24 horas a 30 días.
- Deshabilitar: se deshabilita la mitigación automática del recurso protegido.

6. Recorra el resto de páginas hasta que termine y guarde la configuración.

En la página Protecciones, se actualiza la configuración de mitigación automática del recurso.

Cambio de la acción utilizada para la mitigación automática de DDoS en la capa de aplicación

Puede cambiar la acción que Shield Advanced utiliza para la respuesta automática de la capa de aplicación en varias ubicaciones de la consola:

- Configuración de mitigación automática: cambie la acción al configurar la mitigación automática para su recurso. Para conocer el procedimiento, consulte la sección anterior Cómo habilitar y deshabilitar la mitigación automática de DDoS en la capa de aplicación.
- Página de detalles del evento: cambie la acción en la página de detalles del evento cuando vea la información del evento en la consola. Para obtener más información, consulte AWS Shield Advanced detalles del evento.

Si tiene dos recursos protegidos que comparten una ACL web y establece la acción Count en uno y Block en el otro, Shield Advanced establece la acción de la regla basada en tasas del grupo de reglas `ShieldKnownOffenderIPRateBasedRule` a Block.

Se utiliza AWS CloudFormation con la mitigación automática de DDoS en la capa de aplicación

Aprenda AWS CloudFormation a gestionar sus protecciones y sus ACL AWS WAF web.

Cómo habilitar o deshabilitar la mitigación automática de DDoS en la capa de aplicación

Puede habilitar y deshabilitar la mitigación automática de DDoS en la capa de aplicaciones mediante AWS CloudFormation el `AWS::Shield::Protection` recurso. El efecto es el mismo que cuando se habilita o deshabilita la característica a través de la consola o cualquier otra interfaz. Para obtener información sobre el AWS CloudFormation recurso, consulte AWS::Shield::Protectionla guía del AWS CloudFormation usuario.

Administración de las ACL web utilizadas con mitigación automática

Shield Advanced administra la mitigación automática de su recurso protegido mediante una regla de grupo de reglas en la ACL AWS WAF web del recurso protegido. A través de la AWS WAF consola y las API, verá la regla incluida en las reglas de la ACL web, con un nombre que empieza por`ShieldMitigationRuleGroup`. Esta regla está dedicada a la mitigación automática de DDoS en la capa de aplicación y Shield Advanced y AWS WAF la administran por usted. Para más información, consulte El grupo de reglas de Shield Advanced y Cómo administra Shield Advanced la mitigación automática.

Si lo usa AWS CloudFormation para administrar sus ACL web, no agregue la regla de grupo de reglas Shield Advanced a su plantilla de ACL web. Cuando actualizas una ACL web que se está utilizando con tus protecciones de mitigación automática, administra AWS WAF automáticamente la regla del grupo de reglas en la ACL web.

Verás las siguientes diferencias en comparación con otras ACL web a través AWS CloudFormation de las cuales gestionas:

- AWS CloudFormation no mostrará ningún desfase en el estado de desviación de la pila entre la configuración real de la ACL web, con la regla del grupo de reglas Shield Advanced, y la plantilla de ACL web, sin la regla. La regla de Shield Advanced no aparecerá en los detalles de desviación de la lista del recurso.

  Podrá ver la regla del grupo de reglas Shield Advanced en las listas de ACL web de las que accede, por ejemplo AWS WAF, a través de la AWS WAF consola o AWS WAF las API.
- Si modifica la plantilla de ACL web en una pila AWS WAF y Shield Advanced mantiene automáticamente la regla de mitigación automática de Shield Advanced en la ACL web actualizada. Las protecciones de mitigación automática ofrecidas por Shield Advanced no se ven interrumpidas por la actualización de la ACL web.

No administre la regla Shield Advanced en su plantilla de ACL AWS CloudFormation web. La plantilla de la ACL web no debe incluir la regla de Shield Advanced. Siga las prácticas recomendadas para la administración de ACL web en Prácticas recomendadas para utilizar la mitigación automática.

Detección basada en la salud mediante controles de salud

Puede configurar Shield Advanced para que utilice la detección basada en el estado a fin de mejorar la capacidad de respuesta y la precisión en la detección y mitigación de ataques. Puede usar esta opción con cualquier tipo de recurso, excepto en las zonas alojadas en Route 53.

Para configurar la detección basada en el estado, defina una comprobación de estado de su recurso en Route 53, compruebe que el informe esté en buen estado y, a continuación, asociarla a su protección Shield Advanced. Para obtener información sobre las comprobaciones de estado de Route 53, consulte Cómo comprueba Amazon Route 53 el estado de sus recursos y Cómo crear, actualizar y eliminar las comprobaciones de estado en la Guía para desarrolladores de Amazon Route 53.

> **Note**
>
> Se requieren comprobaciones de estado para poder contar con el apoyo proactivo del equipo de respuesta de Shield (SRT). Para obtener información sobre la interacción proactiva, consulte Configuración de interacción proactiva.

Las comprobaciones de estado miden el estado de los recursos en función de los requisitos que defina. El estado del chequeo de estado proporciona información vital a los mecanismos de detección de Shield Advanced, lo que les da una mayor sensibilidad al estado actual de sus aplicaciones específicas.

Puede habilitar la detección basada en el estado para cualquier tipo de recurso, excepto para las zonas alojadas en Route 53.

- Recursos de la capa de red y transporte (capa 3/capa 4): la detección basada en el estado mejora la precisión de la detección y la mitigación de eventos en las capas de red y transporte para los equilibradores de carga de red, las direcciones IP elásticas y los aceleradores estándar de Global Accelerator. Al proteger estos tipos de recursos con Shield Advanced, Shield Advanced puede proporcionar mitigaciones para ataques más pequeños y una mitigación más rápida para los ataques, incluso cuando el tráfico está dentro de la capacidad de la aplicación.

Cuando agrega la detección basada en estado, durante los períodos en los que la comprobación de estado se registra como en mal estado, Shield Advanced puede aplicar mitigaciones aún más rápidamente y en umbrales más bajos.

- Recursos de la capa de aplicación (capa 7): la detección basada en el estado mejora la precisión de la detección de inundaciones de solicitudes web para CloudFront distribuciones y balanceadores de carga de aplicaciones. Al proteger estos tipos de recursos con Shield Advanced, recibirá alertas de detección de inundaciones por solicitudes web cuando haya una desviación estadísticamente significativa en el volumen de tráfico que se combine con cambios significativos en los patrones de tráfico, según las características de la solicitud.

  Con la detección basada en estado, durante los períodos en que la comprobación de estado de Route 53 asociada se registra como en mal estado, Shield Advanced requiere desviaciones más pequeñas para enviar alertas de los eventos y registrarlos con mayor rapidez. Cuando la comprobación de estado de Route 53 se registra como en buen estado, Shield Advanced requiere desviaciones mayores para enviar alertas.

Contenido

Prácticas recomendadas para utilizar comprobaciones de estado con Shield Advanced

Siga las prácticas recomendadas de esta sección cuando cree y utilice comprobaciones de estado con Shield Advanced.

- Planifique sus comprobaciones de estado identificando los componentes de su infraestructura que desea supervisar. Tenga en cuenta los siguientes tipos de recursos para las comprobaciones de estado:
  - Recursos cruciales.
  - Cualquier recurso en el que desees una mayor sensibilidad en la detección y mitigación de Shield Advanced.
  - Recursos para los que quieres que Shield Advanced se ponga en contacto contigo de forma proactiva. El estado de las comprobaciones de estado se basa en el estado de las comprobaciones de estado.

  Entre los ejemplos de recursos que puede que desee supervisar se incluyen CloudFront las distribuciones de Amazon, los balanceadores de carga con acceso a Internet y las instancias de Amazon EC2.
- Defina comprobaciones de estado que reflejen con precisión el estado del origen de su aplicación con el menor número de notificaciones posible.
  - Realiza comprobaciones de estado para que solo estén en mal estado cuando la aplicación no esté disponible o no funcione dentro de los parámetros aceptables. Es responsable de definir y mantener las comprobaciones de estado en función de los requisitos específicos de su aplicación.
  - Realice el menor número posible de comprobaciones de estado y, al mismo tiempo, informe con precisión sobre el estado de su aplicación. Por ejemplo, varias alarmas de varias áreas de la aplicación que informen sobre el mismo problema podrían sobrecargar sus actividades de respuesta sin añadir valor informativo.
  - Usa controles de estado calculados para monitorear el estado de las aplicaciones mediante una combinación de CloudWatch métricas de Amazon. Por ejemplo, puede calcular el estado combinado en función de la latencia de los servidores de aplicaciones y sus tasas de error de 5 veces mayores, lo que indica que el servidor de origen no atendió la solicitud.
  - Cree y publique sus propios indicadores de estado de la aplicación en métricas CloudWatch personalizadas según sea necesario y utilícelos en una comprobación de estado calculada.
- Implemente y gestione sus comprobaciones de estado para mejorar la detección y reducir las actividades de mantenimiento innecesarias.

- Antes de asociar una comprobación de estado a una protección Shield Advanced, asegúrate de que se encuentre en buen estado. Asociar una comprobación de estado que indique que no está funcionando puede sesgar los mecanismos de detección de Shield Advanced para sus recursos protegidos.
- Mantenga sus controles de salud disponibles para que los utilice Shield Advanced. No elimine una comprobación de estado en Route 53 que esté utilizando para la protección de Shield Advanced.
- Utilice los entornos de ensayo y pruebe únicamente para comprobar sus comprobaciones de estado. Mantenga asociaciones de comprobación de estado únicamente para entornos que requieran un rendimiento y una disponibilidad a nivel de producción. No mantenga una asociación de comprobación de estado en Shield Advanced para los entornos de ensayo y prueba.

Métricas que se utilizan habitualmente para las comprobaciones de estado

En esta sección se enumeran las CloudWatch métricas de Amazon que se utilizan habitualmente en las comprobaciones de estado para medir el estado de las aplicaciones durante los eventos de denegación de servicio distribuido (DDoS). Para obtener información completa sobre las CloudWatch métricas de cada tipo de recurso, consulte la lista que sigue a la tabla.

Temas

Métricas utilizadas en la supervisión el estado de la aplicación

Recurso	Métrica	Descripción
Route 53	`HealthCheckStatus`	El estado del punto de conexión de comprobación de estado.
CloudFront	`5xxErrorRate`	El porcentaje de todas las solicitudes para las que el código de estado de HTTP es 5xx. Esto indica que se

Recurso	Métrica	Descripción
		trata de un ataque que está afectando a la aplicación.
Equilibrador de carga de aplicación	`HTTPCode_ELB_5XX_Count`	El número de códigos de error del cliente HTTP 5xx generados por el balanceador de cargas.
Equilibrador de carga de aplicación	`RejectedConnectionCount`	El número de conexiones que se rechazaron porque el equilibrador de carga alcanzó el número máximo de conexiones.
Equilibrador de carga de aplicación	`TargetConnectionErrorCount`	El número de conexiones que no se establecieron correctamente entre el equilibrador de carga y el destino.
Equilibrador de carga de aplicación	`TargetResponseTime`	El tiempo transcurrido, en segundos, desde que la solicitud abandona el equilibrador de carga hasta que se recibe una respuesta del destino.
Equilibrador de carga de aplicación	`UnHealthyHostCount`	El número de destinos que se considera que no están en buen estado.
Amazon EC2	`CPUUtilization`	El porcentaje de unidades informáticas EC2 asignadas que se usan actualmente.

CloudWatch Métricas de Amazon para cada tipo de recurso

Para obtener información adicional sobre las métricas disponibles para sus recursos protegidos, consulte las siguientes secciones de las guías de recursos:

- Amazon Route 53: monitoriza tus recursos con los controles de estado de Amazon Route 53 y Amazon CloudWatch en la guía para desarrolladores de Amazon Route 53.
- Amazon CloudFront : Monitorización CloudFront con Amazon CloudWatch en la Guía para CloudFront desarrolladores de Amazon.
- Application Load Balancer: CloudWatch métricas de su balanceador de carga de aplicaciones en la guía del usuario de Application Load Balancer.
- Network Load Balancer: CloudWatch métricas de su Network Load Balancer en la Guía del usuario de Network Load Balancer.
- AWS Global Accelerator — Uso de Amazon CloudWatch con AWS Global Accelerator la Guía para AWS Global Accelerator desarrolladores.
- Amazon Elastic Compute Cloud: enumera las CloudWatch métricas disponibles para tus instancias en https://docs.aws.amazon.com/ AWSEC UserGuide 2/latest/ /.
- Amazon EC2 Auto Scaling: supervise CloudWatch las métricas de sus grupos e instancias de Auto Scaling en la Guía del usuario de Auto Scaling de Amazon EC2.

Gestión de las asociaciones de comprobación de estado

Lo que más le beneficiará es utilizar una comprobación de estado con Shield Advanced si la comprobación de estado solo informa de que está en buen estado cuando la aplicación se ejecuta dentro de los parámetros aceptables y solo informa de que está en mal estado cuando no lo está. Utilice las instrucciones de esta sección para gestionar sus asociaciones de comprobación de estado en Shield Advanced.

> **Note**
>
> Shield Advanced no gestiona automáticamente sus comprobaciones de estado.

Para poder realizar una comprobación de estado con Shield Advanced, se requiere lo siguiente:

- La comprobación de estado debe ser correcta cuando la asocie a su protección Shield Advanced.

- La comprobación de estado debe ser relevante para el estado de su recurso protegido. Es responsable de definir y mantener las comprobaciones de estado que informen con precisión sobre el estado de su aplicación, en función de los requisitos específicos de la aplicación.
- La comprobación de estado debe permanecer disponible para que la utilice la protección Shield Advanced. No elimine una comprobación de estado en Route 53 que esté utilizando para la protección de Shield Advanced.

Temas

Asociar una comprobación de estado a su recurso

El procedimiento siguiente muestra cómo asociar una comprobación de estado de Amazon Route 53 a una protección.

> **Note**
>
> Antes de asociar una comprobación de estado a una protección Shield Advanced, asegúrate de que se encuentre en buen estado. Para obtener información, consulte Supervisión del estado de las comprobaciones de estado y recepción de notificaciones en la Guía para desarrolladores de Amazon Route 53.

Asociación de una comprobación de estado

1. Inicie sesión en la AWS Management Console consola AWS WAF & Shield y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel AWS Shield de navegación, elija Recursos protegidos.
3. En la pestaña Protecciones, seleccione el recurso que desee asociar a una comprobación de estado.
4. Elija Configurar las protecciones.
5. Seleccione Siguiente hasta llegar a la página Configurar la detección de DDoS basada en comprobaciones de estado opcional.

6. En Associated Health Check (Comprobación de estado asociada), elija el identificador de la comprobación de estado que desea asociar a la protección.

   > **Note**
   >
   > Si no ve la comprobación de estado que necesita, vaya a la consola de Route 53 y verifique la comprobación de estado y su ID. Para obtener más información, consulte Creación y actualización de comprobaciones de estado.

7. Recorra el resto de las páginas hasta que termine la configuración. En la página de Protecciones, aparece la asociación de comprobación de estado actualizada del recurso.
8. En la página de Protecciones, compruebe que la comprobación de estado que acaba de asociar esté funcionando correctamente.

   No puede empezar a utilizar correctamente una comprobación de estado en Shield Advanced mientras la comprobación de estado indica que no funciona correctamente. Si lo hace, Shield Advanced detecta falsos positivos en umbrales muy bajos y también puede afectar negativamente a la capacidad del equipo de respuesta de Shield (SRT) de interactuar proactivamente con el recurso.

   Si la nueva comprobación de estado asociada indica que no es correcto, haga lo siguiente:

   a. Desvincule la comprobación de estado de su protección en Shield Advanced.
   b. Revisite las especificaciones de las comprobaciones de estado en Amazon Route 53 y compruebe el rendimiento y la disponibilidad generales de la aplicación.
   c. Cuando su aplicación funcione dentro de sus parámetros de buen estado y su comprobación de estado informe que funciona correctamente, intente de nuevo asociar la comprobación de estado en Shield Advanced.

El procedimiento de asociación de comprobación de estado estará completo cuando haya establecido su nueva asociación de comprobación de estado y se notifique que está en buen estado en Shield Advanced.

Desasociar una comprobación de estado de su recurso

El siguiente procedimiento muestra cómo desasociar una comprobación de estado de Amazon Route 53 de un recurso protegido.

Desasociación de una comprobación de estado

1. Inicie sesión en la AWS Management Console consola AWS WAF & Shield y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel AWS Shield de navegación, elija Recursos protegidos.
3. En la pestaña Protecciones, seleccione el recurso que desee desasociar de una comprobación de estado.
4. Elija Configurar las protecciones.
5. Seleccione Siguiente hasta llegar a la página Configurar la detección de DDoS basada en comprobaciones de estado opcional.
6. En comprobación de estado asociada, elija la opción vacía, que aparece como -.
7. Recorra el resto de las páginas hasta que termine la configuración.

En la página Protecciones, el campo de comprobación de estado del recurso está establecido en -, lo que indica que no hay ninguna asociación de comprobación de estado.

El estado de la asociación de comprobación de estado

Puede ver el estado de la comprobación de estado asociada a una protección en la página de recursos protegidos de la consola de Shield AWS WAF y en la página de detalles de cada recurso.

- Saludable: la comprobación de estado está disponible y se indica que es correcto.
- Insalubre: la comprobación de estado está disponible y se indica que no es saludable.
- No disponible: Shield Advanced no puede utilizar la comprobación de estado.

Para resolver una comprobación de estado no disponible

Crear y utilizar una nueva comprobación de estado. No intente volver a asociar una comprobación de estado después de que haya tenido el estado de no disponible en Shield Advanced.

Para obtener instrucciones detalladas acerca de cómo seguir estos pasos, consulte los temas anteriores.

1. En Shield Advanced, desasocie la comprobación de estado del recurso.
2. A continuación, en Route 53, cree una nueva comprobación de estado para la protección y anote su ID. Para obtener información, consulte Creación y actualización de comprobaciones de estado en la Guía para desarrolladores de Amazon Route 53.

3. En Shield Advanced, asociamos la comprobación de estado nueva con el recurso.

Ejemplos de comprobación de estado

En esta sección se muestran ejemplos de comprobaciones de estado que puede utilizar en una comprobación de estado calculada. Una comprobación de estado calculada utiliza una serie de comprobaciones de estado individuales para determinar un estado combinado. El estado de cada control de estado individual se basa en el estado de un punto final o en el estado de una CloudWatch métrica de Amazon. Las comprobaciones de estado se combinan en un control de estado calculado y, a continuación, se configura el control de estado calculado para informar sobre el estado de salud en función del estado de salud combinado de las comprobaciones de estado individuales. Ajuste la sensibilidad de las comprobaciones de estado calculadas en función de sus requisitos de rendimiento y disponibilidad de las aplicaciones.

Para obtener información sobre las comprobaciones de estado calculadas, consulte Supervisión de otras comprobaciones de estado (comprobaciones de estado calculadas) en la Guía para desarrolladores de Amazon Route 53. Para obtener información adicional, consulte la entrada del blog Route 53 Improvements: Calculated Health Checks and Latency Checks.

Temas

- CloudFront Distribuciones de Amazon
- Equilibradores de carga
- Dirección IP elástica (EIP) de Amazon EC2

CloudFront Distribuciones de Amazon

Los siguientes ejemplos describen los controles de estado que podrían combinarse en un control de estado calculado para una CloudFront distribución:

- Supervise un punto de conexión especificando un nombre de dominio en una ruta de la distribución que ofrece contenido dinámico. Una respuesta correcta incluiría los códigos de respuesta HTTP 2xx y 3xx.
- Supervisa el estado de una CloudWatch alarma que mide el estado del CloudFront origen. Por ejemplo, puede mantener una CloudWatch alarma en la métrica `TargetResponseTime` Application Load Balancer y crear una comprobación de estado que refleje el estado de la alarma. La comprobación de estado puede no funcionar correctamente cuando el tiempo de respuesta,

entre la solicitud que sale del equilibrador de carga y el momento en que el equilibrador de carga recibe una respuesta del objetivo, supera el umbral configurado en la alarma.

- Supervisa el estado de una CloudWatch alarma que mide el porcentaje de solicitudes para las que el código de estado HTTP de la respuesta es 5xx. Si la tasa de error de 5xx de la CloudFront distribución es superior al umbral definido en la CloudWatch alarma, el estado de esta comprobación de estado pasará a ser insalubre.

Equilibradores de carga

Los siguientes ejemplos describen las comprobaciones de estado que podrían usarse en las comprobaciones de estado calculadas para un acelerador estándar del Equilibrador de carga de aplicación, Equilibrador de carga de red o Global Accelerator.

- Supervise el estado de una CloudWatch alarma que mide la cantidad de nuevas conexiones establecidas por los clientes al balanceador de carga. Puede establecer el umbral de alarma para el número medio de conexiones nuevas en un grado superior al promedio diario. Las métricas para cada tipo de recurso son las siguientes:
  - Equilibrador de carga de aplicación: `NewConnectionCount`
  - Equilibrador de carga de red: `ActiveFlowCount`
  - Global Accelerator: `NewFlowCount`
- En el caso de Application Load Balancer y Network Load Balancer, supervise el estado de CloudWatch una alarma que mida la cantidad de balanceadores de carga que se consideran en buen estado. Puede configurar el umbral de alarma en la zona de disponibilidad o en la cantidad mínima de hosts en buen estado que requiere el equilibrador de carga. Las métricas disponibles para los recursos del equilibrador de carga son las siguientes:
  - Equilibrador de carga de aplicación: `HealthyHostCount`
  - Equilibrador de carga de red: `HealthyHostCount`
- En el caso de Application Load Balancer, supervise el estado de una CloudWatch alarma que mida la cantidad de códigos de respuesta HTTP 5xx generados por los objetivos del balanceador de carga. Para un Equilibrador de carga de aplicación, puede usar la métrica `HTTPCode_Target_5XX_Count` y basar el umbral de alarma en la suma de todos los 5xx errores del equilibrador de carga.

Dirección IP elástica (EIP) de Amazon EC2

Los siguientes ejemplos de comprobaciones de estado podrían combinarse en una comprobación de estado calculada para una dirección IP elástica de Amazon EC2:

- Para supervisar un punto de conexión, especifique una dirección IP para la dirección IP elástica. La comprobación de estado se mantendrá en buen estado siempre que se pueda establecer una conexión TCP con el recurso detrás de la dirección IP.
- Supervise el estado de una CloudWatch alarma que mide el porcentaje de unidades informáticas de Amazon EC2 asignadas que se utilizan actualmente en la instancia. Puede usar la métrica Amazon EC2 `CPUUtilization` y basar el umbral de alarma en lo que considere una tasa de utilización de la CPU alta para su aplicación, como el 90 %.

Gestión de la protección de los recursos en AWS Shield Advanced

Utilice las instrucciones de esta sección para administrar las protecciones Shield Advanced de sus recursos.

> **Note**
>
> Shield Advanced protege solo los recursos que haya especificado en Shield Advanced o mediante una política de AWS Firewall Manager Shield Advanced. No protege automáticamente sus recursos.

Si utilizas una política AWS Firewall Manager Shield Advanced, no necesitas gestionar las protecciones de los recursos que están dentro del ámbito de aplicación de la política. Firewall Manager administra automáticamente las protecciones de las cuentas y los recursos que están dentro del ámbito de una política, de acuerdo con la configuración de la política. Para obtener más información, consulte AWS Shield Advanced políticas.

Temas

- Añadir AWS Shield Advanced protección a AWS los recursos
- Configuración de AWS Shield Advanced las protecciones
- Eliminar AWS Shield Advanced la protección de un AWS recurso

Añadir AWS Shield Advanced protección a AWS los recursos

Sigue las instrucciones de esta sección para añadir la protección Shield Advanced a uno o más recursos.

Para añadir protección a un AWS recurso

1. Inicie sesión en la AWS Management Console consola AWS WAF & Shield y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel de navegación, AWS Shield seleccione Recursos protegidos.
3. Seleccione Añadir recursos para proteger.
4. En la página Elegir los recursos que se protegerán con Shield Advanced, en Especificar la región y los tipos de recursos, proporcione las especificaciones de región y de tipo de recurso de los recursos que desea proteger. Puede proteger los recursos de varias regiones seleccionando Todas las regiones y puede limitar la selección a los recursos globales seleccionando Global. Puede deseleccionar cualquier tipo de recurso que no desee proteger. Para obtener información sobre las protecciones de sus tipos de recursos, consulte AWS Shield Advanced protecciones por tipo de recurso.
5. Elija Cargar recursos. Shield Advanced rellena la sección Seleccionar recursos con los recursos de AWS que coinciden con sus criterios.
6. En la sección Seleccionar recursos, puede filtrar la lista de recursos introduciendo una cadena para buscarla en las listas de recursos.

   Seleccione los recursos que desea proteger.
7. En la sección Etiquetas, si desea agregar etiquetas a las protecciones Shield Advanced que está creando, especifíquelas. Para obtener información acerca de cómo etiquetar los recursos de AWS , consulte Uso de Tag Editor.
8. Elija Proteger con Shield Advanced. Esto agrega las protecciones de Shield Advanced a los recursos.

Configuración de AWS Shield Advanced las protecciones

Puede cambiar la configuración de sus AWS Shield Advanced protecciones en cualquier momento. Para ello, debe recorrer las opciones de todas las protecciones seleccionadas y modificar la configuración que necesite cambiar.

Administración de recursos protegidos

1. Inicie sesión en la AWS Management Console consola AWS WAF & Shield y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel AWS Shield de navegación, elija Recursos protegidos.
3. En la pestaña Protecciones, seleccione los recursos que desea proteger.
4. Elija Configurar las protecciones y la opción de especificación de recursos que desee.
5. Revise cada una de las opciones de protección de recursos y realice los cambios necesarios.

Configure las protecciones DDoS en la capa de aplicación

Para protegerse contra los ataques a los recursos de Amazon CloudFront y Application Load Balancer, puede añadir ACL AWS WAF web y reglas basadas en tasas. Para obtener más información acerca de este tema, consulte Shield: ACL AWS WAF web de capa de aplicación avanzada y reglas basadas en tasas.

También puede habilitar la mitigación de DDoS automática de la capa de aplicación de Shield Advanced. Para obtener información sobre cómo AWS WAF funciona, consulte. AWS WAF Para obtener información sobre la característica de mitigación automática, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced.

> **Important**
>
> Si administra sus protecciones de Shield Advanced AWS Firewall Manager mediante una política de Shield Advanced, no podrá administrar las protecciones de la capa de aplicación aquí. Para todos los demás recursos, recomendamos que, como mínimo, adjunte una ACL web a cada recurso, incluso si la ACL web no contiene ninguna regla.

> **Note**
>
> Cuando habilita la mitigación automática de DDoS en la capa de aplicación para un recurso, si es necesario, la operación agrega automáticamente un rol vinculado a un servicio a su cuenta para otorgar a Shield Advanced los permisos que necesita para administrar sus protecciones de ACL web. Para obtener más información, consulte Uso de roles vinculados a servicios para Shield Advanced.

Configuración de las protecciones DDoS a nivel de aplicación

1. En la página Configurar las protecciones DDoS de capa 7, si el recurso aún no está asociado a una ACL web, puede elegir una ACL web existente o crear la suya propia.

   Para crear una ACL web, siga estos pasos:

   a. Elija Create web ACL (Crear ACL web).

   b. Escriba un nombre. No se puede cambiar el nombre después de crear la ACL web.

   c. Seleccione Crear.

   > **Note**
   >
   > Si un recurso ya está asociado a una ACL web, no puede cambiar a otra ACL web. Si desea cambiar la ACL, primero debe eliminar las ACL web asociadas del recurso. Para obtener más información, consulte Asociar o desasociar una ACL web a un recurso AWS.

2. Si la ACL web no tiene definida una regla basada en la velocidad, puede agregar una. Para ello, seleccione Añadir regla basada en tasas y, a continuación, lleve a cabo los siguientes pasos:

   a. Escriba un nombre.

   b. Escriba un límite de frecuencia. Esta es la cantidad máxima de solicitudes permitidas en cualquier período de cinco minutos desde cualquier dirección IP antes de que se aplique la acción de regla basada en tasas a la dirección IP. Cuando las solicitudes de la dirección IP caen por debajo del límite, la acción se interrumpe.

   c. Establezca la acción de regla para contar o bloquear solicitudes de direcciones IP cuando sus recuentos de solicitudes superen el límite. La acción de aplicación y eliminación de la regla puede tener efecto uno o dos minutos después de que cambie la tasa de solicitudes de direcciones IP.

   d. Seleccione Añadir regla.

3. Para la mitigación automática de DDoS en la capa de aplicaciones, elija si quiere que Shield Advanced mitigue automáticamente los ataques DDoS en su nombre, de la siguiente manera:

   - Para activar la mitigación automática, elija Activar y, a continuación, seleccione la acción de AWS WAF regla que quiere que Shield Advanced utilice en sus reglas personalizadas. Sus opciones son Count y Block. Para obtener información sobre estas acciones de AWS

WAF regla, consulteAcción de regla. Para obtener información sobre cómo Shield Advanced administra esta configuración de acción, consulte Cómo Shield Advanced administra la configuración de acciones de las reglas.

- Para deshabilitar la mitigación automática, seleccione Desactivar.
- Para dejar la configuración de mitigación automática sin cambios para los recursos que está administrando, deje la opción predeterminada Mantener la configuración actual.

Para obtener información sobre la mitigación de DDoS automática de la capa de aplicación de Shield Advanced, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced.

4. Elija Siguiente.

Creación de alarmas y notificaciones

El siguiente procedimiento muestra cómo gestionar CloudWatch las alarmas de los recursos protegidos.

> **Note**
>
> CloudWatch incurre en costes adicionales. Para CloudWatch conocer los precios, consulta Amazon CloudWatch Pricing.

Creación de notificaciones y alarmas de Amazon

1. En la página de protecciones Crear alarmas y notificaciones de Amazon CloudWatch (opcional), configure los temas de SNS para las alarmas y notificaciones que desea recibir. Para los recursos para los que no desea recibir notificaciones, elija Ningún tema. Puede añadir un tema de Amazon SNS o crear uno nuevo.
2. Para crear un tema de Amazon SNS, siga estos pasos:

   a. En la lista desplegable, seleccione Crear nuevo tema.

   b. Escriba un nombre de tema.

   c. Opcionalmente, escriba una dirección de correo electrónico a la que se enviarán los mensajes de Amazon SNS y, a continuación, elija Añadir dirección de correo electrónico. Puede introducir más de una.

d. Seleccione Crear.

3. Elija Siguiente.

Eliminar AWS Shield Advanced la protección de un AWS recurso

Puede eliminar AWS Shield Advanced la protección de cualquiera de sus AWS recursos en cualquier momento.

> **Important**
>
> Al eliminar un AWS recurso, no se elimina el recurso de AWS Shield Advanced. También debe quitar la protección del recurso AWS Shield Advanced, tal y como se describe en este procedimiento.

Quitar AWS Shield Advanced la protección de un AWS recurso

1. Inicie sesión en la AWS Management Console consola AWS WAF & Shield y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel AWS Shield de navegación, elija Recursos protegidos.
3. En la pestaña Protecciones, seleccione los recursos cuyas protecciones desee eliminar.
4. Elija Eliminar protección.

   - Si tienes una CloudWatch alarma de Amazon configurada como protección, tienes la opción de eliminar la alarma junto con la protección. Si decides no eliminar la alarma en este momento, puedes eliminarla más adelante mediante la CloudWatch consola.

   > **Note**
   >
   > En el caso de las protecciones que tienen configurada una comprobación de estado de Amazon Route 53, si agrega la protección de nuevo más adelante, la protección seguirá incluyendo la comprobación de estado.

Los pasos anteriores eliminan AWS Shield Advanced la protección de AWS recursos específicos. No cancelan tu AWS Shield Advanced suscripción. Se le seguirá cobrando por el servicio. Para obtener

información sobre su AWS Shield Advanced suscripción, póngase en contacto con el AWS Support Centro.

Eliminar una CloudWatch alarma de las protecciones Shield Advanced

Para eliminar una CloudWatch alarma de las protecciones Shield Advanced, realice una de las siguientes acciones:

- Elimine la protección como se describe en Eliminar AWS Shield Advanced la protección de un AWS recurso. Asegúrese de seleccionar la casilla de verificación situada junto a Also delete related DDoSDetection alarm (Eliminar también la alarma de DDoSDetection correspondiente).
- Elimine la alarma con la CloudWatch consola. El nombre de la alarma que se va a eliminar comienza con DDoS DetectedAlarmForProtection.

AWS Shield Advanced grupos de protección

Use los grupos de protección para crear colecciones lógicas de sus recursos protegidos y administre sus protecciones como un grupo. Para obtener más información sobre la administración de los recursos de protección, consulte Configuración de AWS Shield Advanced las protecciones.

> **Note**
>
> La mitigación automática de DDoS en la capa de aplicación no interactúa con los grupos de protección. Puede habilitar la mitigación automática para los recursos que se encuentran en grupos de protección, pero Shield Advanced no aplica automáticamente mitigaciones de ataques en función de los hallazgos de los grupos de protección. Shield Advanced aplica mitigaciones de ataque automáticas a recursos individuales.

AWS Shield Advanced Los grupos de protección le ofrecen una forma de autoservicio de personalizar el alcance de la detección y la mitigación al tratar varios recursos protegidos como una sola unidad. La agrupación de recursos puede ofrecer una serie de ventajas.

- Mejore la precisión de la detección.
- Reduzca las notificaciones de eventos no procesables.
- Aumente la cobertura de las acciones de mitigación para incluir los recursos protegidos que también podrían verse afectados durante un evento.

- Acelere el tiempo necesario para mitigar los ataques con varios objetivos similares.
- Facilite la protección automática de los recursos protegidos recién creados.

Los grupos de protección pueden ayudar a reducir los falsos positivos en situaciones como el cambio entre valores azules y verdes, en los que los recursos se alternan entre estar prácticamente sin carga o estar completamente cargados. Otro ejemplo es cuando creas y eliminas recursos con frecuencia y, al mismo tiempo, mantienes un nivel de carga que comparten los miembros del grupo. En situaciones como estas, la supervisión de los recursos individuales puede generar falsos positivos, mientras que la supervisión del estado del grupo de recursos no.

Puede configurar los grupos de protección para que incluyan todos los recursos protegidos, todos los recursos de tipos de recursos específicos o los recursos especificados individualmente. Los recursos recién protegidos que cumplen los criterios del grupo de protección se incluyen automáticamente en el grupo de protección. Un recurso protegido puede pertenecer a varios grupos de protección.

Administración de grupos AWS Shield Advanced de protección

Utilice las instrucciones de esta sección para administrar las configuraciones de grupos de protección.

Creación de un grupo de protección Shield Advanced

Creación de un grupo de protección

1. Inicie sesión en la AWS Management Console consola AWS WAF & Shield y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel AWS Shield de navegación, elija Recursos protegidos.
3. Seleccione la pestaña Grupos de protección y, a continuación, seleccione Crear grupo de protección.
4. En la página Crear grupo de protección, proporcione un nombre para el grupo. Utilizará este nombre para identificar el grupo en su lista de recursos protegidos. No puede cambiar el nombre de un grupo de protección después de crearlo.
5. En cuanto a los Criterios de agrupamiento de Protection, seleccione los criterios que desee que Shield Advanced utilice para identificar los recursos protegidos que desee incluir en el grupo. Realice las selecciones adicionales en función de los criterios que haya elegido.
6. En Agregar, seleccione cómo quiere que Shield Advanced combine los datos de recursos del grupo para detectar, mitigar e informar sobre los eventos.

- Sumar: utilice el tráfico total del grupo. Es una buena opción para la mayoría de los casos. Los ejemplos incluyen direcciones IP elásticas para instancias de Amazon EC2 que se escalan manual o automáticamente.
- Media: utilice el promedio del tráfico en todo el grupo. Esta es una buena opción para los recursos que comparten el tráfico de manera uniforme. Algunos ejemplos son los aceleradores y los equilibradores de carga.
- Máximo: utilice el tráfico más alto de cada recurso. Esto resulta útil para los recursos que no comparten tráfico y para los recursos que lo comparten de forma no uniforme. Algunos ejemplos son CloudFront las distribuciones de Amazon y los recursos de origen para las CloudFront distribuciones.

7. Elija Guardar para guardar el grupo de protección y volver a la página de Recursos protegidos.

En la página Eventos Shield, puede ver los eventos de su grupo de protección y profundizar para ver información adicional sobre los recursos protegidos que están en el grupo.

Actualización de un grupo de protección Shield Advanced

Actualización de un grupo de protección

1. Inicie sesión en la AWS Management Console consola AWS WAF & Shield y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel AWS Shield de navegación, elija Recursos protegidos.
3. En la pestaña Grupos de protección, active la casilla de verificación situada al lado del grupo de protección que desea modificar.
4. En la página del grupo de protección, seleccione Editar. Realice los cambios que desee en la configuración del grupo de protección.
5. Elija Guardar para guardar los cambios.

Eliminación de un grupo de protección de Shield Advanced

Eliminación de un grupo de protección

1. Inicie sesión en la AWS Management Console consola AWS WAF & Shield y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel AWS Shield de navegación, elija Recursos protegidos.

3. En la pestaña Grupos de protección, active la casilla de verificación situada al lado del grupo de protección que desea eliminar.
4. En la página del grupo de protección, seleccione Eliminar y confirme la acción.

Seguimiento de los cambios en la protección de los recursos en AWS Config

Puede registrar los cambios en la AWS Shield Advanced protección de sus recursos utilizando AWS Config. A continuación, puede utilizar esta información para mantener un historial de cambios de configuración para auditoría y solución de problemas.

Para registrar los cambios de protección, AWS Config habilítelos para cada recurso del que desee realizar un seguimiento. Para obtener más información, consulte Introducción a AWS Config en la Guía para desarrolladores de AWS Config .

Debe habilitarlo AWS Config para cada uno de los Región de AWS que contengan los recursos rastreados. Puede activarlos AWS Config manualmente o utilizar la AWS CloudFormation plantilla «Activar AWS Config» en la sección Plantillas de AWS CloudFormation StackSets muestra de la Guía del AWS CloudFormation usuario.

Si la habilitas AWS Config, se te cobrará tal y como se detalla en la página de AWS Config precios.

> **Note**
>
> Si ya has AWS Config activado las regiones y los recursos necesarios, no necesitas hacer nada. AWS Config los registros relacionados con los cambios de protección de sus recursos comienzan a rellenarse automáticamente.

Tras activarla AWS Config, utilice la región EE.UU. Este (Virginia del Norte) de la AWS Config consola para ver el historial de cambios de configuración de los recursos AWS Shield Advanced globales.

Consulte el historial de cambios de los recursos AWS Shield Advanced regionales a través de la AWS Config consola en las regiones EE.UU. Este (Norte de Virginia), EE.UU. Este (Ohio), EE.UU. Oeste (Oregón), EE.UU. Oeste (Norte de California), Europa (Irlanda), Europa (Fráncfort), Asia Pacífico (Tokio) y Asia Pacífico (Sídney).

Visibilidad de los eventos de DDoS

AWS Shield proporciona visibilidad de las siguientes categorías de eventos y actividades de eventos:

- Global: todos los clientes pueden acceder a una visión agregada de la actividad de las amenazas globales durante las últimas dos semanas. Puede consultar esta información en las páginas de introducción y del panel de control de amenazas globales de la AWS Shield consola. Para obtener más información, consulte AWS Shield actividad global y de cuentas.
- Cuenta: todos los clientes pueden acceder a un resumen de los eventos de su cuenta durante el año anterior. Puede ver esta información en la página de introducción de la AWS Shield consola. Para obtener más información, consulte AWS Shield actividad global y de cuentas.

Cuando se suscribe a Shield Advanced y añade protecciones a sus recursos, obtiene acceso a información adicional sobre los eventos y los ataques DDoS a los recursos protegidos:

- Eventos sobre recursos protegidos: Shield Advanced proporciona información detallada de cada evento a través de la página Eventos de la AWS Shield consola. Para obtener más información, consulte AWS Shield Advanced eventos.
- Métricas de eventos para recursos protegidos: Shield Advanced publica las CloudWatch métricas de detección, mitigación y principales contribuyentes de Amazon para todos los recursos que protege. Puede utilizar estas métricas para configurar CloudWatch paneles y alarmas. Para obtener más información, consulte AWS Shield Advanced métricas.
- Visibilidad de eventos entre cuentas para recursos protegidos: si utiliza AWS Firewall Manager para administrar sus protecciones de Shield Advanced, puede habilitar la visibilidad de las protecciones en varias cuentas mediante el uso combinado AWS Security Hub de Firewall Manager. Para obtener más información, consulte Visibilidad de eventos en cuentas.

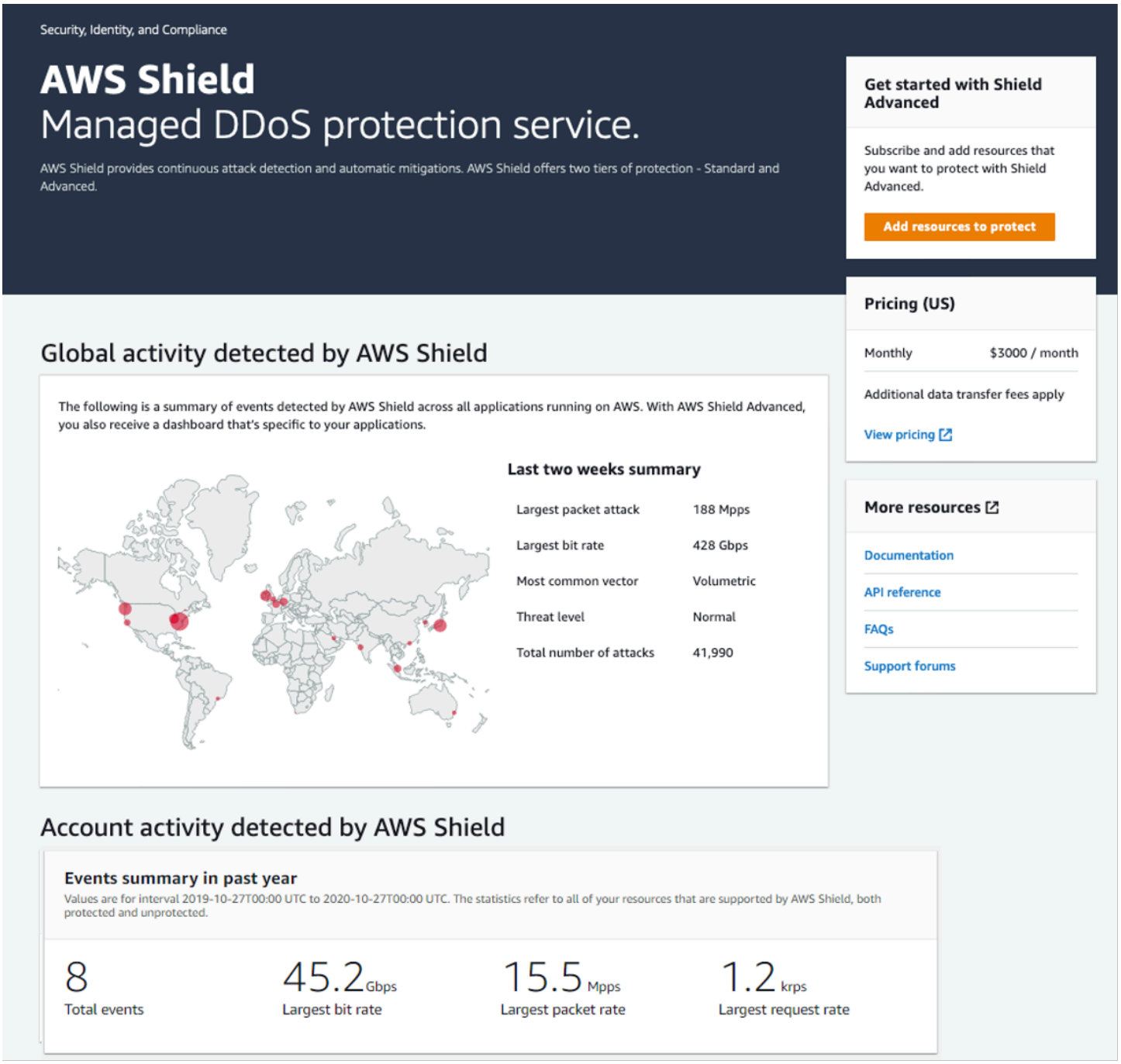
Si habilita la mitigación automática de DDoS en la capa de aplicación para una protección en la capa de aplicación,

Temas

AWS Shield actividad global y de cuentas

Puede acceder a una vista global de la actividad de las amenazas globales y a un resumen de los eventos por cuenta en las páginas de introducción y del panel de control de amenazas globales de la AWS Shield consola.

En la siguiente captura de pantalla se muestra un ejemplo de la página de Introducción.



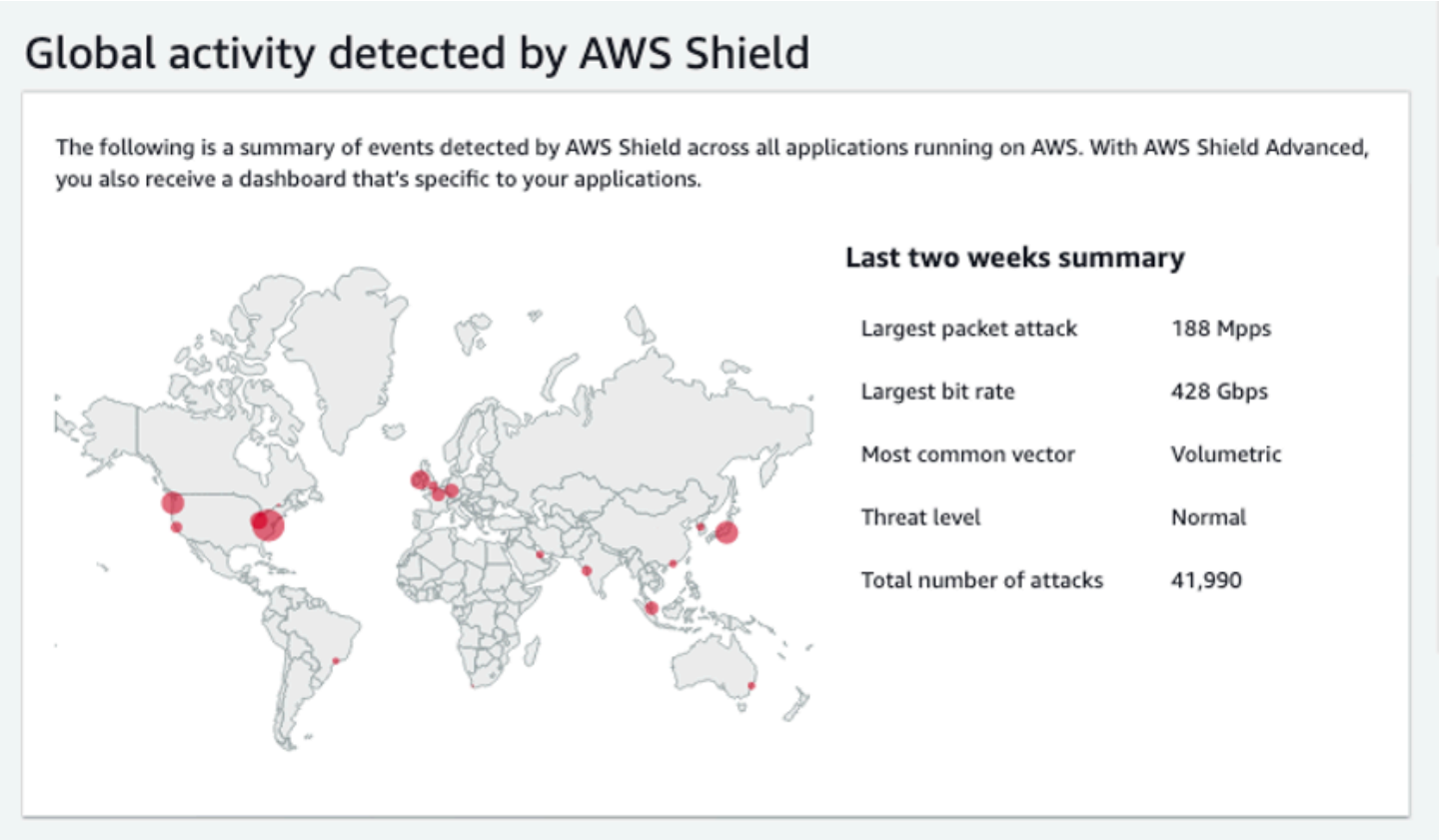
Para acceder a la AWS Shield consola

- Inicie sesión en la AWS Management Console consola AWS WAF & Shield y ábrala en https://console.aws.amazon.com/wafv2/.

No necesita una suscripción a Shield Advanced para acceder a la información resumida de actividades globales y los eventos de las cuentas.

Actividad global

Esta información está disponible en el panel global de amenazas de la AWS Shield consola y en las páginas de introducción. En la siguiente captura de pantalla se muestra un ejemplo del panel de actividades globales.



La actividad global describe los eventos de DDoS observados en todos los clientes. AWS Una vez por hora, AWS actualiza la información de las dos semanas anteriores. En el panel de la consola, puedes ver los resultados, divididos por AWS región y mostrados en un mapa térmico mundial. Junto al mapa, Shield muestra información resumida, como el mayor ataque de paquetes, la mayor velocidad de bits, el vector más común, el número total de ataques y el nivel de amenaza. El nivel de amenaza es una evaluación de la actividad global actual en comparación con lo que AWS suele

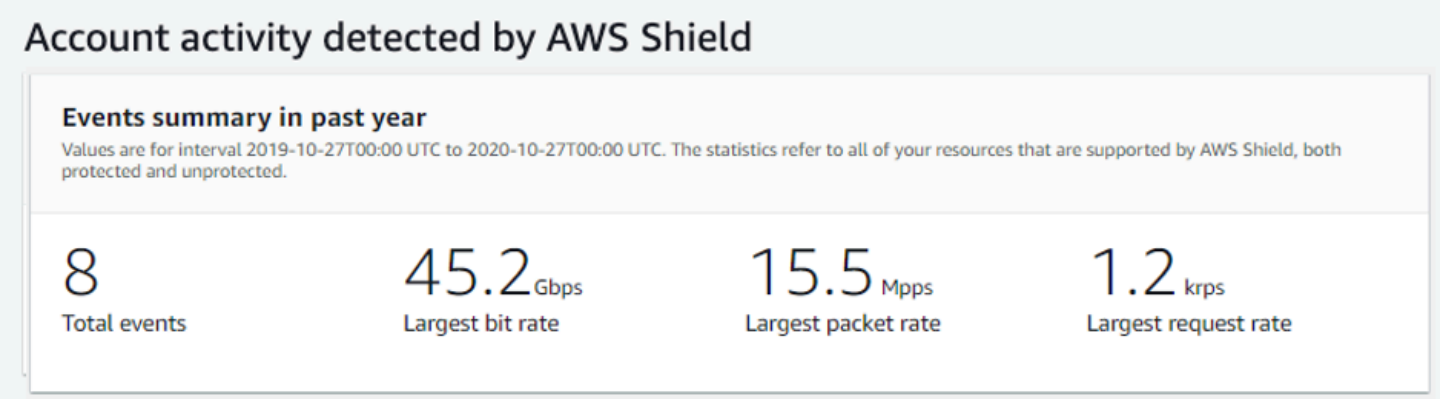
observar. El valor predeterminado del nivel de amenaza es Normal. AWS actualiza automáticamente el valor a Alto para una actividad DDoS elevada.

El Panel de amenazas globales también proporciona métricas de series temporales y le permite cambiar entre períodos de tiempo. Para ver el historial de los ataques DDoS más importantes, puede personalizar el panel para ver las vistas desde el último día hasta las dos últimas semanas. Las métricas de series temporales proporcionan una vista de la velocidad de bits, la velocidad de paquetes o la tasa de solicitudes más altas de todos los eventos detectados AWS Shield por las aplicaciones que se estén ejecutando AWS durante el período de tiempo que seleccione.

Actividad de la cuenta

Esta información está disponible en la página de introducción de la AWS Shield consola.

En la siguiente captura de pantalla se muestra un ejemplo del panel de actividades de la cuenta.



La actividad de la cuenta describe los eventos de DDoS que Shield detectó para sus recursos y que son aptos para la protección de Shield Advanced. Todos los días, Shield crea métricas resumidas para el año que finalizó a las 00:00 UTC del día anterior y, a continuación, muestra el total de eventos, la velocidad de bits más alta, la velocidad de paquetes más alta y la tasa de solicitudes más alta.

- La métrica total de eventos refleja cada vez que Shield detectó atributos sospechosos en el tráfico destinado a su aplicación. Los atributos sospechosos pueden incluir tráfico con un volumen superior al normal, tráfico que no coincida con el perfil histórico de la aplicación o tráfico que no coincida con las heurísticas definidas por Shield para el tráfico de aplicaciones válido.
- Las estadísticas de mayor velocidad de bits y mayor velocidad de paquetes están disponibles para cada recurso.

- La estadística de mayor tasa de solicitudes solo está disponible para CloudFront las distribuciones de Amazon y los balanceadores de carga de aplicaciones que tienen una ACL web asociada AWS WAF .

> **Note**
>
> También puede acceder al resumen de eventos a nivel de cuenta a través de la operación de la AWS Shield API. DescribeAttackStatistics

AWS Shield Advanced eventos

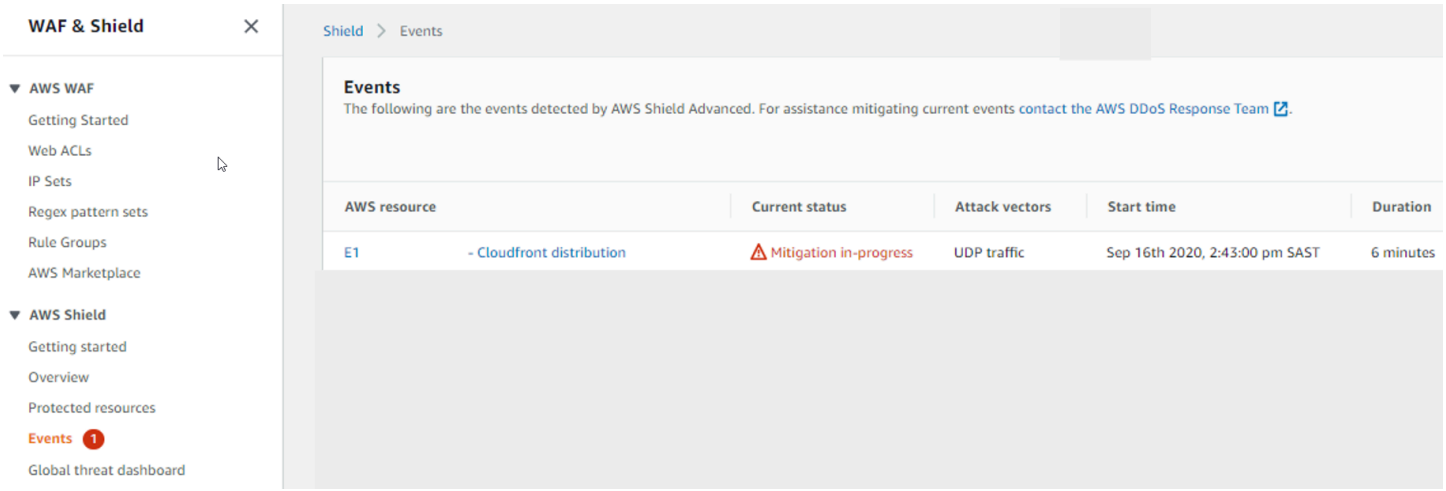
Cuando se suscribe a Shield Advanced y protege sus recursos, obtiene acceso a características de visibilidad adicionales para los recursos. Estos incluyen notificaciones casi en tiempo real de los eventos detectados por Shield Advanced e información adicional sobre los eventos detectados y las mitigaciones.

> **Note**
>
> La información de tus eventos en la consola de Shield Advanced se basa en las métricas de Shield Advanced. Para obtener información sobre las métricas de Shield Advanced, consulte AWS Shield Advanced métricas

AWS Shield evalúa el tráfico hacia su recurso protegido en varias dimensiones. Cuando se detecta una anomalía, Shield Advanced crea un evento independiente para cada recurso afectado.

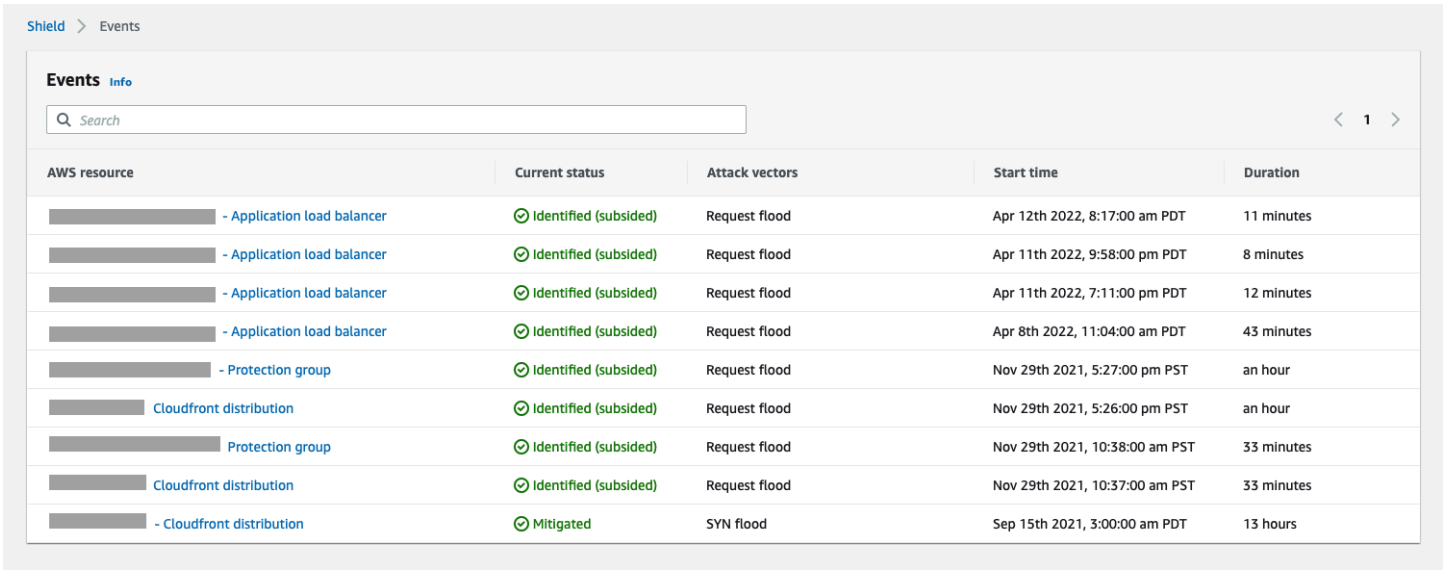
Puede acceder a los resúmenes y detalles de los eventos a través de la página Eventos de la consola de Shield. La página Eventos de nivel superior proporciona una descripción general de los eventos actuales y pasados.

En la siguiente captura de pantalla se muestra un ejemplo de página de Eventos con un único evento en curso. Este evento activo también está marcado en el panel de navegación izquierdo.



Shield Advanced también puede aplicar automáticamente mitigaciones contra los ataques, según el tipo de tráfico y las protecciones configuradas. Estas medidas de mitigación pueden evitar que su recurso reciba tráfico excesivo o tráfico que coincida con una firma de ataque DDoS conocida.

La siguiente captura de pantalla muestra un ejemplo de una lista Eventos de todos los eventos que Shield Advanced mitigó o que disminuyeron por sí solos.



Proteja sus recursos antes de un evento

Mejore la precisión de la detección de eventos protegiendo los recursos con Shield Advanced mientras reciben el tráfico normal esperado, antes de que sean objeto de un ataque DDoS.

Para informar con precisión de los eventos de un recurso protegido, Shield Advanced debe establecer primero una referencia de los patrones de tráfico que se esperan para ese recurso.

- Shield Advanced informa de los eventos de la capa de infraestructura de los recursos después de que hayan estado protegidos durante al menos 15 minutos.
- Shield Advanced informa de los eventos de la capa de aplicación web para recursos después de que hayan estado protegidos durante al menos 24 horas. La precisión de la detección de los eventos de la capa de aplicación es mejor después de que Shield Advanced haya observado el tráfico esperado durante 30 días.

Para acceder a la información de los eventos en la AWS Shield consola

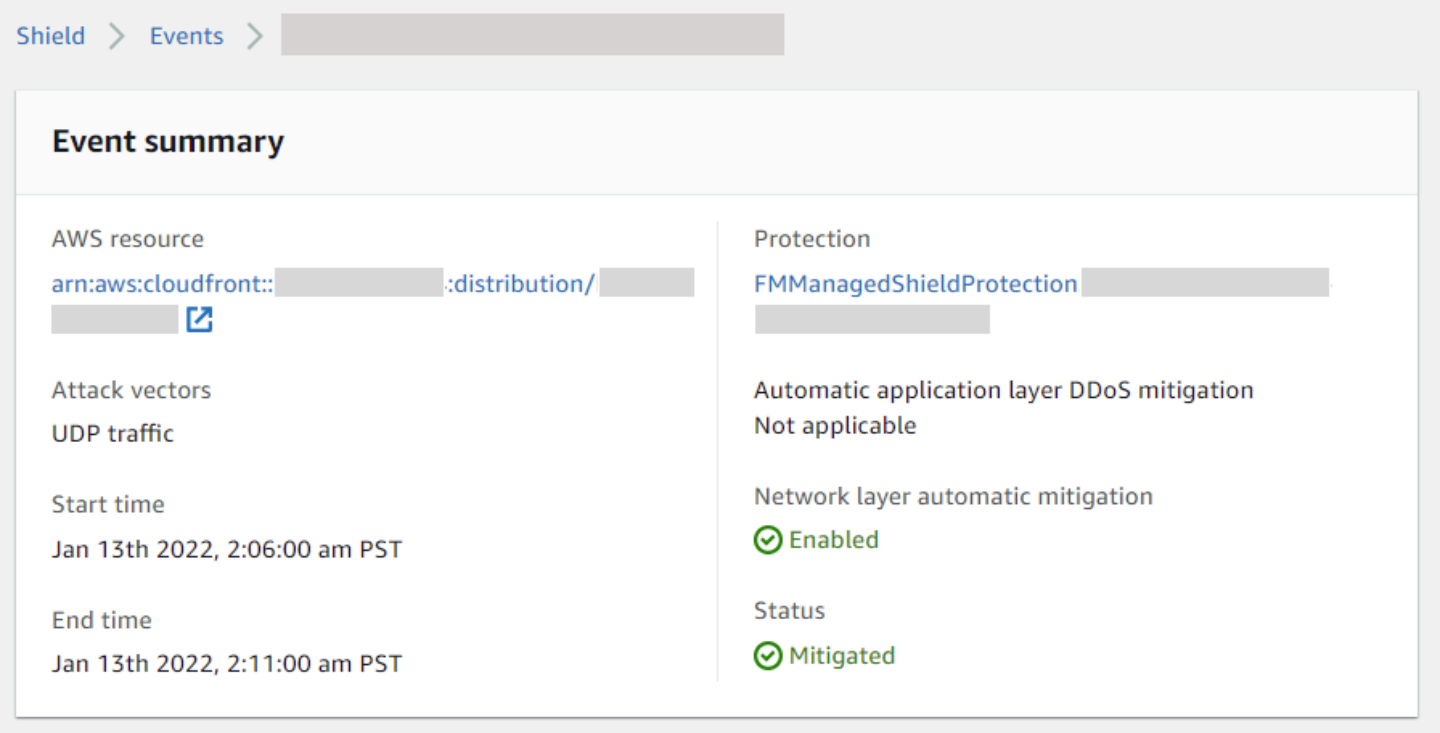
1. Inicie sesión en la AWS Management Console consola AWS WAF & Shield y ábrala en https://console.aws.amazon.com/wafv2/.
2. En el panel AWS Shield de navegación, elija Eventos. La consola muestra la página Eventos.
3. En la página Eventos, puede seleccionar cualquier evento de la lista para ver información resumida adicional y detalles del evento.

Temas

AWS Shield Advanced resúmenes de eventos

Puede ver el resumen y la información detallada de un evento en la página de consola del evento. Para abrir la página de un evento, seleccione el nombre del AWS recurso en la lista de páginas de eventos.

En la siguiente captura de pantalla se muestra un ejemplo de resumen de un evento de capa de red.



La información del resumen de la página del evento incluye la siguiente información.

- Estado actual: valores que indican el estado del evento y las acciones que Shield Advanced ha realizado en el evento. Los valores de estado se aplican a los eventos de la capa de infraestructura (capa 3 o 4) y de la capa de aplicación (capa 7).
  - Identificado (en curso) e Identificado (disminuido): indican que Shield Advanced detectó un evento, pero no ha tomado ninguna medida al respecto hasta el momento. Identificado (disminuido): indica que el tráfico sospechoso que detectó Shield se detuvo sin intervención.
  - Mitigación en curso y Mitigado: indican que Shield Advanced detectó un evento y ha tomado medidas al respecto. Mitigation también se usa cuando el recurso objetivo es una CloudFront distribución de Amazon o una zona alojada en Amazon Route 53, que tienen sus propias mitigaciones integradas automáticas.
- Vectores de ataque: vectores de ataque DDoS, como las saturaciones de TCP SYN, y las heurísticas de detección de Shield Advanced, como las saturaciones de solicitudes. Estos pueden indicar un ataque DDoS.
- Hora de inicio: fecha y hora en que se detectó el primer punto de datos de tráfico anómalos.
- Duración u hora de finalización: indica el tiempo transcurrido entre la hora de inicio del evento y el último punto de datos anómalos observado por Shield Advanced. Mientras un evento esté en curso, estos valores seguirán aumentando.

- Protección: nombra la protección de Shield Advanced que está asociada al recurso y proporciona un enlace a su página de protección. Esto está disponible en la página del evento individual.
- Mitigación automática de DDoS en la capa de aplicación: se utiliza para la protección de la capa de aplicación, para indicar si la mitigación automática de DDoS en la capa de aplicación de Shield Advanced está habilitada para el recurso. Si se habilita, proporciona un enlace para acceder a la configuración y administrarla. Esto está disponible en la página del evento individual.
- Mitigación automática de la capa de red: indica si el recurso tiene una mitigación automática en la capa de red. Si un recurso tiene un componente de capa de red, lo tendrá habilitado. Esta información está disponible en la página del evento individual.

En el caso de los recursos a los que se dirige con frecuencia, Shield puede implementar mitigaciones una vez que se haya reducido el exceso de tráfico, para evitar que se repitan más eventos.

> **Note**
>
> También puede acceder a los resúmenes de eventos de los recursos protegidos a través de la operación de la API. AWS Shield ListAttacks

AWS Shield Advanced detalles del evento

Puede ver los detalles sobre la detección y mitigación de un evento y los principales colaboradores en la sección inferior de la página de la consola correspondiente al evento. Esta sección puede incluir una combinación de tráfico legítimo y potencialmente no deseado, y puede representar tanto el tráfico que se ha transferido a su recurso protegido como el tráfico que ha sido bloqueado por las mitigaciones de Shield.

- Detección y mitigación: proporciona información sobre el evento observado y cualquier medida de mitigación aplicada al mismo. Para obtener información acerca de la mitigación de eventos, consulte Respuesta a eventos de DDoS.
- Principales colaboradores: clasifica el tráfico implicado en el evento y enumera los principales orígenes del tráfico que Shield ha identificado para cada categoría. En el caso de los eventos de la capa de aplicación, utilice la información de los principales colaboradores para hacerse una idea general de la naturaleza de un evento, pero utilice los AWS WAF registros para tomar decisiones de seguridad. Para obtener más información, consulte las secciones siguientes.

La información de tus eventos en la consola de Shield Advanced se basa en las métricas de Shield Advanced. Para obtener información sobre las métricas de Shield Advanced, consulte AWS Shield Advanced métricas

Las métricas de mitigación no se incluyen para los recursos de Amazon CloudFront o Amazon Route 53, ya que estos servicios están protegidos por un sistema de mitigación que siempre está habilitado y no requiere mitigaciones para los recursos individuales.

Las secciones de detalles varían en función de si la información corresponde a un evento de la capa de infraestructura o de la capa de aplicación.

Detalles de evento de la capa de aplicación

Puede ver los detalles sobre la detección y mitigación de un evento de la capa de aplicación y los principales colaboradores en la sección inferior de la página de la consola correspondiente al evento. Esta sección puede incluir una combinación de tráfico legítimo y potencialmente no deseado, y puede representar tanto el tráfico que se ha transferido a su recurso protegido como el tráfico que ha sido bloqueado por las mitigaciones de Shield Advanced.

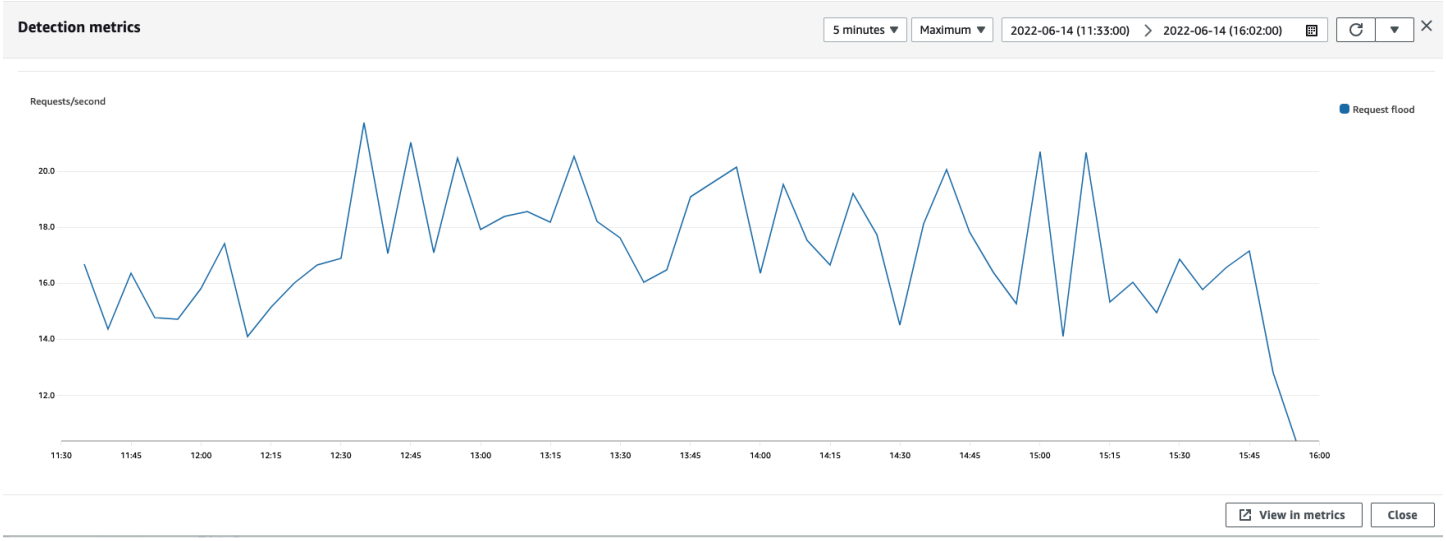
Los detalles de la mitigación se refieren a cualquier regla de la ACL web que esté asociada al recurso, incluidas las reglas que se implementan específicamente en respuesta a un ataque y las reglas basadas en la velocidad que se definen en la ACL web. Si habilita la mitigación automática de DDoS en la capa de aplicación para una aplicación, las métricas de mitigación incluyen las métricas de esas reglas adicionales. Para obtener información sobre estas protecciones de la capa de aplicación, consulteAWS Shield Advanced protecciones de capa de aplicación (capa 7).

Detección y mitigación

Para un evento de capa de aplicación (capa 7), la pestaña Detección y mitigación muestra las métricas de detección que se basan en la información obtenida de los AWS WAF registros. Las métricas de mitigación se basan en las reglas de AWS WAF de la ACL web asociada que están configuradas para bloquear el tráfico no deseado.

En el caso de CloudFront las distribuciones de Amazon, puedes configurar Shield Advanced para que te aplique mitigaciones automáticas. Con cualquier recurso de capa de aplicación, se puede elegir definir reglas de mitigación propias en la ACL web y solicitar ayuda al equipo de respuesta de Shield (SRT). Para obtener información sobre estas opciones, consulte Respuesta a eventos de DDoS.

En la siguiente captura de pantalla se muestra un ejemplo de las métricas de detección de un evento de la capa de aplicaciones que desapareció después de varias horas.



El tráfico de eventos que disminuye antes de que entre en vigor una regla de mitigación no se representa en las métricas de mitigación. Esto puede provocar una diferencia entre el tráfico de solicitudes web que se muestra en los gráficos de detección y las métricas de permiso y bloqueo que se muestran en los gráficos de mitigación.

Colaboradores principales

La pestaña Colaboradores principales de los eventos de la capa de aplicación muestra los 5 principales contribuyentes que Shield ha identificado para el evento, en función de los AWS WAF registros que ha recuperado. Shield clasifica la información de los principales contribuyentes por dimensiones, como la IP de origen, el país de origen y la URL de destino.

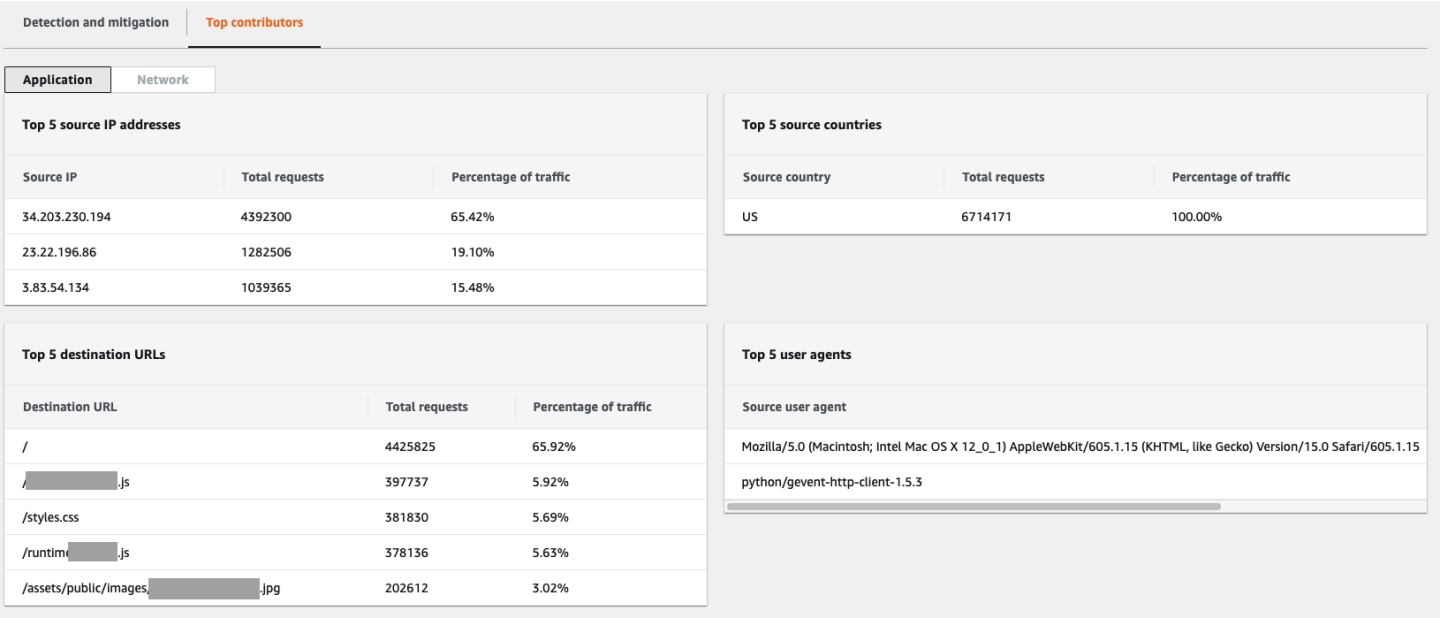
> **Note**
>
> Para obtener la información más precisa sobre el tráfico que contribuye a un evento de la capa de aplicaciones, utilice los AWS WAF registros.

Utilice la información de los principales colaboradores de la capa de aplicación de Shield solo para hacerse una idea general de la naturaleza de un ataque y no base sus decisiones de seguridad en ella. En el caso de los eventos de la capa de aplicación, los AWS WAF registros son la mejor fuente de información para comprender los factores que contribuyen a un ataque y para diseñar sus estrategias de mitigación.

La información de los principales colaboradores de The Shield no siempre refleja completamente los datos de los AWS WAF registros. Cuando incorpora los registros, Shield prioriza la reducción

del impacto en el rendimiento del sistema en vez de recuperar todos los datos de los registros. Esto puede provocar una pérdida del grado de detalle en los datos que estén disponibles para que Shield los analice. En la mayoría de los casos, la mayor parte de la información está disponible, pero es posible que los datos de los principales contribuyentes estén sesgados hasta cierto punto debido a un ataque.

En la siguiente captura de pantalla se muestra un ejemplo de la pestaña de Colaboradores principales en un evento de capa de aplicación.



La información de los colaboradores se basa en las solicitudes de tráfico legítimo y potencialmente no deseado. Los eventos de mayor volumen y los eventos en los que los orígenes de solicitudes no están muy distribuidos tienen más probabilidades de tener colaboradores principales identificables. Un ataque muy distribuido puede tener múltiples orígenes, lo que dificulta la identificación de los principales contribuyentes al ataque. Si Shield Advanced no identifica a los contribuyentes importantes de una categoría específica, muestra los datos como no disponibles.

Detalles de evento de la capa de infraestructura

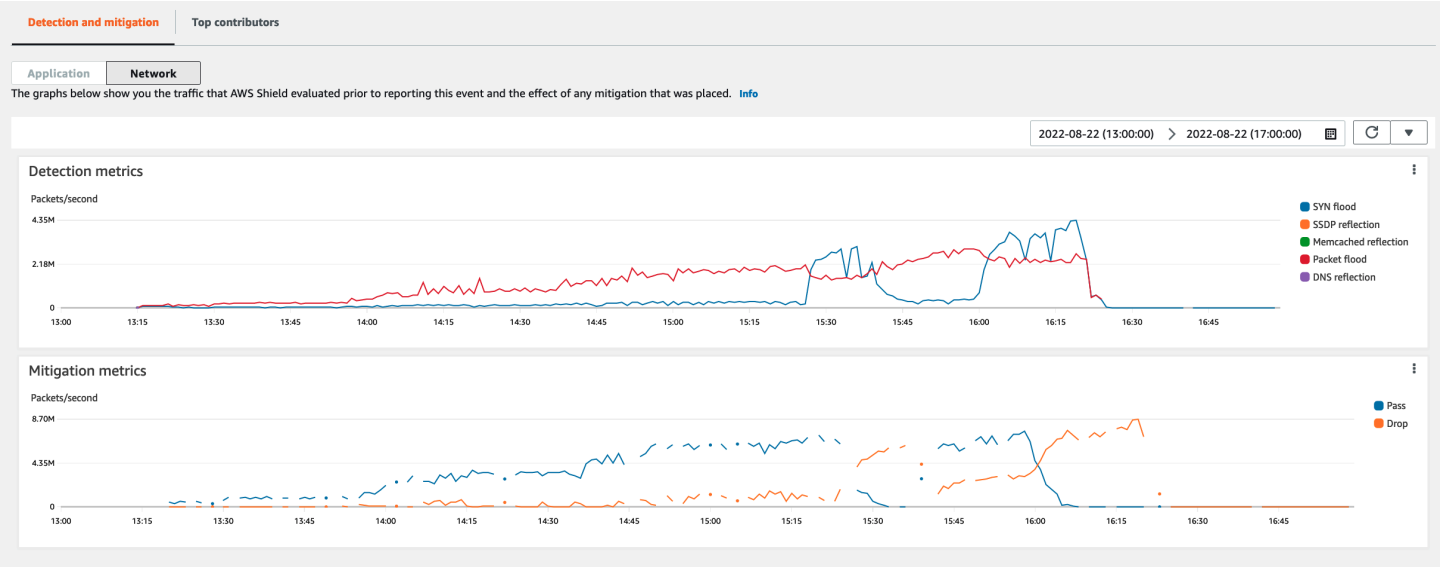
Puede ver los detalles sobre la detección y mitigación de un evento de la capa de la infraestructura, y los principales colaboradores en la sección inferior de la página de la consola correspondiente al evento. Esta sección puede incluir una combinación de tráfico legítimo y potencialmente no deseado, y puede representar tanto el tráfico que se ha transferido a su recurso protegido como el tráfico que ha sido bloqueado por las mitigaciones de Shield.

Detección y mitigación

En el caso de un evento de capa de infraestructura (capa 3 o 4), la pestaña Detección y mitigación muestra las métricas de detección que se basan en flujos de red muestreados y las métricas de mitigación que se basan en el tráfico observado por los sistemas de mitigación. Las métricas de mitigación son una medida más precisa del tráfico que llega a su recurso.

Shield crea automáticamente una mitigación para los tipos de recursos protegidos Elastic IP (EIP), Classic Load Balancer (CLB), Application Load Balancer (ALB) y Standard Accelerator. AWS Global Accelerator Las métricas de mitigación de las direcciones EIP y los aceleradores AWS Global Accelerator estándar indican la cantidad de paquetes aprobados y descartados.

La siguiente captura de pantalla muestra un ejemplo de la pestaña Detección y mitigación para un evento de la capa de infraestructura.

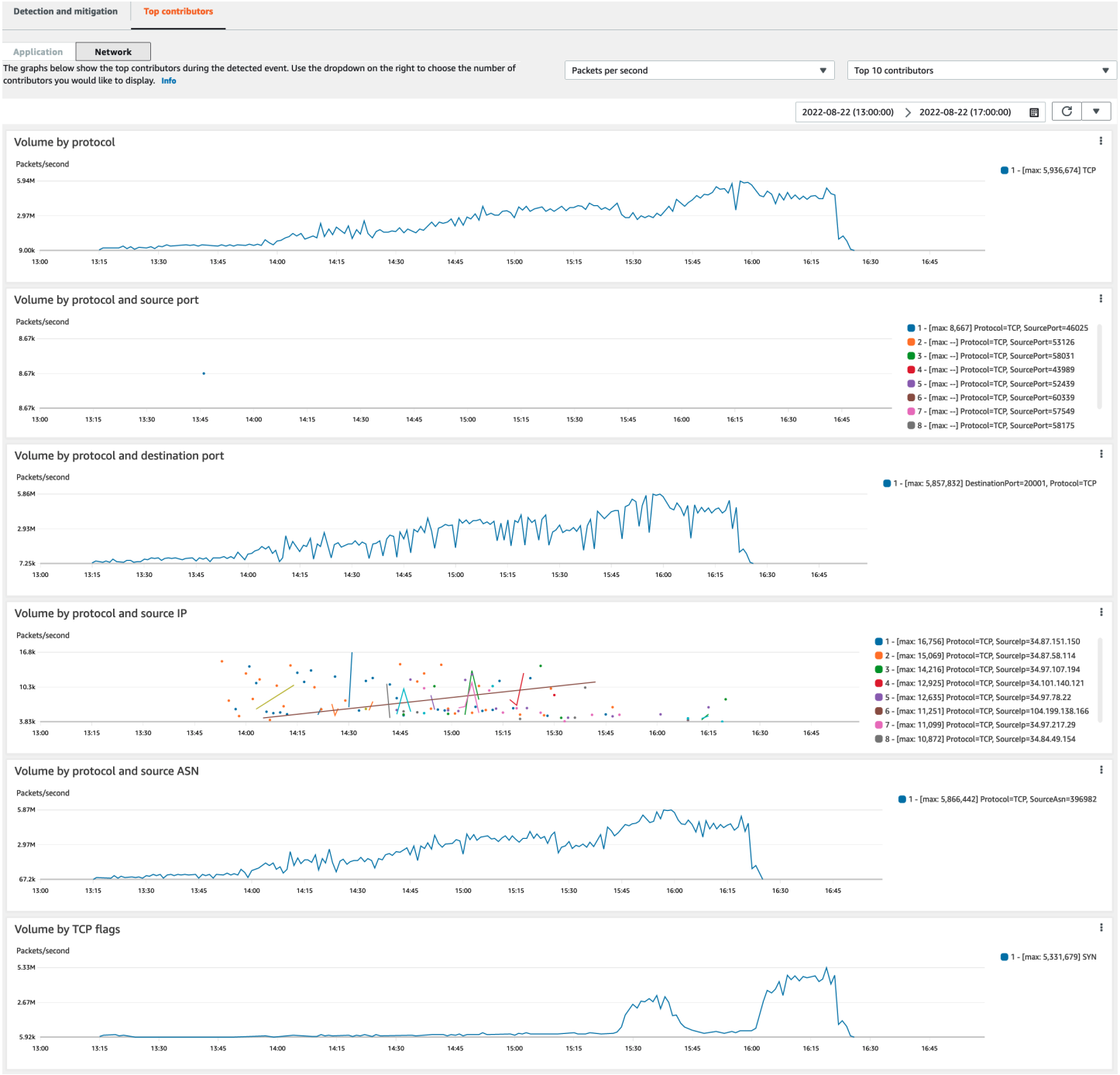


El tráfico de eventos que disminuye antes de que Shield aplique una mitigación no se representa en las métricas de mitigación. Esto puede provocar una diferencia entre el tráfico que se muestra en los gráficos de detección y las métricas de permiso y bloqueo que se muestran en los gráficos de mitigación.

Colaboradores principales

La pestaña Colaboradores principales para eventos de la capa de infraestructura enumera las métricas de hasta 100 colaboradores principales en varias dimensiones del tráfico. Los detalles incluyen las propiedades de la capa de red para cualquier dimensión en la que se puedan identificar al menos cinco orígenes de tráfico importantes. Algunos ejemplos de orígenes de tráfico son la IP de origen y el ASN de origen.

En la siguiente captura de pantalla se muestra un ejemplo de pestaña de Colaboradores principales en un evento de capa de infraestructura.



Las métricas de colaboradores se basan en flujos de red muestreados, tanto para el tráfico legítimo como para el potencialmente no deseado. Los eventos de mayor volumen y los eventos en los que los orígenes de tráfico no están muy distribuidos tienen más probabilidades de tener colaboradores principales identificables. Un ataque muy distribuido puede tener múltiples orígenes, lo que dificulta la identificación de los principales contribuyentes al ataque. Si Shield no identifica a

ningún contribuyente importante de una categoría o métrica específica, muestra los datos como no disponibles.

En un ataque DDoS a nivel de infraestructura, los orígenes del tráfico pueden estar suplantados o reflejados. Un origen suplantado ha sido falsificado a propósito por el atacante. Un origen reflejado es el verdadero origen del tráfico detectado, pero no participa voluntariamente en el ataque. Por ejemplo, un atacante podría generar un gran flujo de tráfico amplificado hacia un objetivo a base de reflejar el ataque en servicios de Internet que, por lo general, son legítimos. En este caso, la información del origen puede ser válida aunque no sea el origen real del ataque. Estos factores pueden limitar la viabilidad de las técnicas de mitigación que bloquean los orígenes en función de los encabezados de paquetes.

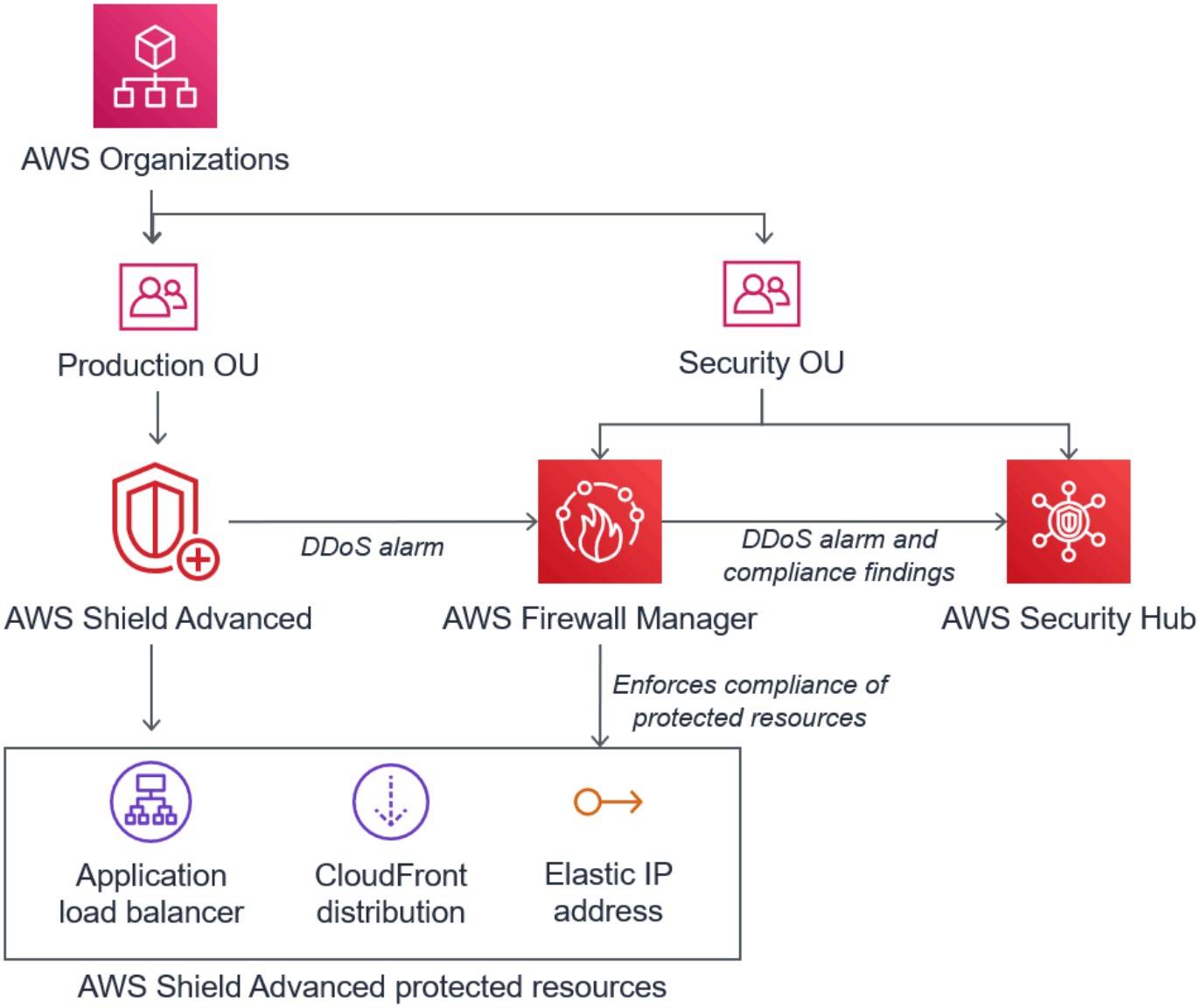
Visibilidad de eventos en cuentas

Puede usar, AWS Security Hub administrar AWS Firewall Manager y monitorear los recursos AWS Shield Advanced protegidos en varias cuentas.

Con Firewall Manager, puede crear una política de seguridad de Shield Advanced que informe e imponga el cumplimiento de la protección frente a DDoS en todas las cuentas. Firewall Manager supervisa sus recursos protegidos e incluye la incorporación de protecciones a los nuevos recursos que entran dentro de la política de Shield Advanced.

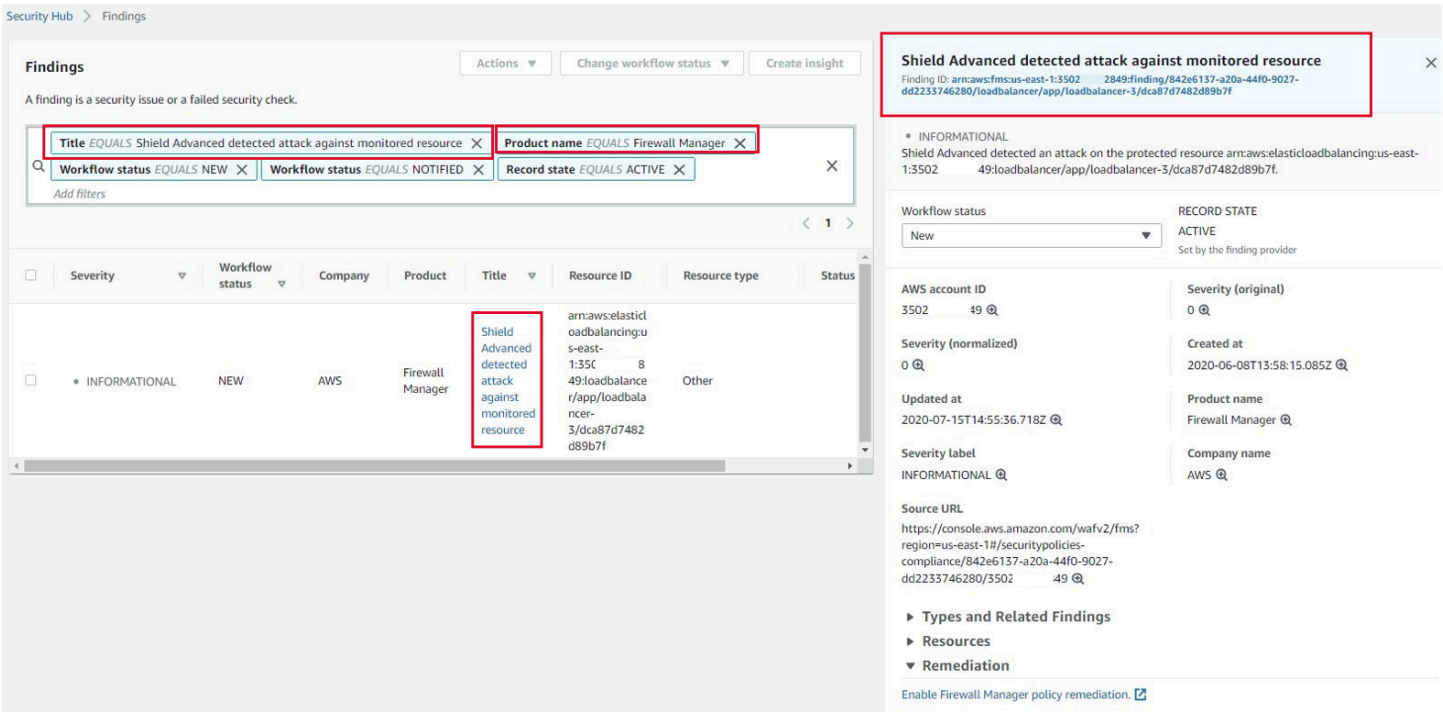
Puede integrar Firewall Manager AWS Security Hub para obtener un panel único que informe de los eventos de DDoS detectados por los resultados de cumplimiento de Shield Advanced y Firewall Manager, cuando Firewall Manager identifica un recurso que no cumple con su política de seguridad de Shield Advanced.

La siguiente figura muestra una arquitectura típica para supervisar los recursos protegidos de Shield Advanced con Firewall Manager y Security Hub.



Al integrar Firewall Manager en Security Hub, se pueden ver los resultados de seguridad en un solo lugar, junto con otras alertas e información sobre el estado de cumplimiento de las aplicaciones en las que se ejecuta AWS.

La siguiente captura de pantalla resalta la información que se puede ver sobre un evento de Shield Advanced en la consola de Security Hub cuando se tiene una integración de este tipo.



Para obtener información sobre cómo integrar Firewall Manager y Security Hub con Shield Advanced para centralizar la supervisión de eventos y el cumplimiento en todas sus cuentas protegidas, consulte el blog de AWS seguridad Configure la supervisión centralizada de los eventos de DDoS y corrija automáticamente los recursos que no cumplan con las normas.

Respuesta a eventos de DDoS

AWS mitiga automáticamente los ataques de denegación de servicio distribuido (DDoS) de red y transporte (capa 3 y capa 4). Si utiliza Shield Advanced para proteger sus instancias de Amazon EC2, durante un ataque, Shield Advanced despliega automáticamente las ACL de la red de Amazon VPC en el borde de la red de AWS . Esto permite a Shield Advanced brindar protección contra eventos de DDoS de mayor envergadura. Para obtener más información acerca de las ACL de red, consulte ACL de red.

En el caso de los ataques DDoS en la capa de aplicación (capa 7), AWS intenta detectar y notificar a AWS Shield Advanced los clientes mediante alarmas. CloudWatch De forma predeterminada, no aplica mitigaciones automáticamente para evitar bloquear inadvertidamente el tráfico de usuarios válidos.

En el caso de los recursos de la capa de aplicación (capa 7), dispone de las siguientes opciones para responder a un ataque.

- Proporcionar sus propias mitigaciones: puede investigar y mitigar el ataque por su cuenta. Para obtener más información, consulte Mitigación manual de un ataque DDoS en la capa de aplicación.
- Ponerse en contacto con el servicio de asistencia: si es cliente de Shield Advanced, puede ponerse en contacto con el Centro de AWS Support para obtener ayuda con las mitigaciones. Los casos críticos y urgentes se redirigen directamente a expertos DDoS. Para obtener más información, consulte Cómo ponerse en contacto con el centro de soporte durante un ataque DDoS en la capa de aplicación.

Además, antes de que se produzca un ataque, puede activar de forma proactiva las siguientes opciones de mitigación:

- Mitigaciones automáticas en las CloudFront distribuciones de Amazon: con esta opción, Shield Advanced define y gestiona las reglas de mitigación para usted en su ACL web. Para obtener información sobre la mitigación automática de la capa de aplicaciones, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced.
- Interacción proactiva: cuando AWS Shield Advanced detecta un ataque de gran tamaño en la capa de aplicación contra una de sus aplicaciones, el SRT puede ponerse en contacto con usted de forma proactiva. El SRT clasifica el evento de DDoS y crea mitigaciones de AWS WAF . El SRT se pone en contacto con usted y, con su consentimiento, puede aplicar las reglas de AWS WAF . Para obtener más información acerca de esta opción, consulte Configuración de interacción proactiva.

Cómo ponerse en contacto con el centro de soporte durante un ataque DDoS en la capa de aplicación

Si es AWS Shield Advanced cliente, puede ponerse en contacto con el AWS Support Centro para obtener ayuda con las mitigaciones. Los casos críticos y urgentes se redirigen directamente a expertos DDoS. De AWS Shield Advanced este modo, los casos complejos se pueden remitir al AWS Shield Response Team (SRT), que tiene una amplia experiencia en la protección AWS de Amazon.com y sus subsidiarias. Para obtener más información sobre SRT, consulte Asistencia del equipo de respuesta de Shield (Shield Response Team, SRT).

Para obtener asistencia del equipo de respuesta de Shield (SRT), póngase en contacto con el Centro de AWS Support. El tiempo de respuesta de su caso depende de la gravedad que seleccione y los tiempos de respuesta, que están documentados en la página Planes de AWS Support.

Seleccione las siguientes opciones:

- Tipo de caso: soporte técnico
- Servicio: denegación de servicio distribuido (DDoS)
- Categoría: Entrante a AWS
- Gravedad: elija la opción correspondiente

Cuando hable con nuestro representante, explíquele que es un AWS Shield Advanced cliente que está siendo objeto de un posible ataque DDoS. Nuestro representante remitirá su llamada a los expertos DDoS adecuados. Si abre un caso con el Centro de AWS Support mediante el tipo de servicio Denegación de servicio distribuido (DDoS), puede hablar directamente con un experto en DDoS a través del chat o por teléfono. Los ingenieros de soporte de DDoS pueden ayudarlo a identificar los ataques, recomendar mejoras en su AWS arquitectura y brindarle orientación sobre el uso de los AWS servicios para mitigar los ataques DDoS.

En el caso de los ataques en la capa de aplicación, el SRT puede ayudarle a analizar la actividad sospechosa. Si tiene habilitada la mitigación automática para su recurso, el SRT puede revisar las mitigaciones que Shield Advanced aplica automáticamente contra el ataque. En cualquier caso, el SRT puede ayudarle a revisar y mitigar el problema. Las medidas de mitigación que recomienda la SRT suelen requerir que la SRT cree o actualice listas de control de acceso a la AWS WAF web (ACL web) en su cuenta. El SRT necesitará su permiso para realizar este trabajo.

> **Important**
>
> Te recomendamos que, como parte de la activación AWS Shield Advanced, sigas los pasos que se indican Configuración del acceso para el equipo de respuesta de Shield (SRT) a continuación para proporcionar al SRT de forma proactiva los permisos que necesita para ayudarte durante un ataque. Proporcionar permiso de antemano ayuda a evitar retrasos si se produce un ataque real.

El SRT le ayuda a clasificar el ataque DDoS para identificar firmas y patrones de ataque. Con tu consentimiento, el SRT crea e implementa AWS WAF reglas para mitigar el ataque.

También puede ponerse en contacto con el SRT antes o durante un posible ataque para revisar mitigaciones y desarrollar e implementar mitigaciones personalizadas. Por ejemplo, si ejecuta una

aplicación web y solo necesita tener abiertos los puertos 80 y 443, puede trabajar con el SRT para preconfigurar una ACL web que permita ("allow") únicamente los puertos 80 y 443.

Debe autorizar y contactar con el SRT en el nivel de cuenta. Es decir, si utiliza Shield Advanced en una política de Shield Advanced de Firewall Manager, es el propietario de la cuenta, no el administrador de Firewall Manager, quien debe ponerse en contacto con el SRT para solicitar asistencia. El administrador de Firewall Manager puede contactar con el SRT solo para las cuentas de las que sea propietario.

Mitigación manual de un ataque DDoS en la capa de aplicación

Si determina que la actividad de la página de eventos de su recurso representa un ataque DDoS, puede crear sus propias AWS WAF reglas en su ACL web para mitigar el ataque. Esta es la única opción disponible si no eres cliente de Shield Advanced. AWS WAF se incluye sin AWS Shield Advanced coste adicional. Para obtener información sobre la creación de reglas en su ACL web, consulte AWS WAF listas de control de acceso web (ACL web).

Si las usa AWS Firewall Manager, puede agregar sus AWS WAF reglas a una AWS WAF política de Firewall Manager.

Cómo mitigar manualmente un ataque DDoS en la posible capa de aplicación

1. Cree declaraciones de reglas en su ACL web con criterios que coincidan con el comportamiento inusual. Para empezar, configúrelas para que cuenten las solicitudes coincidentes. Para obtener información sobre la configuración de la ACL web y las declaraciones de reglas, consulte Evaluación de reglas y grupos de reglas de ACL web y Probando y ajustando sus AWS WAF protecciones.

   > **Note**
   >
   > Pruebe siempre primero las reglas; para ello, utilice inicialmente la acción de regla Count en lugar de Block. Cuando tenga la seguridad de que sus nuevas reglas identifican las solicitudes correctas, puede modificarlas para bloquear las solicitudes.

2. Supervise los recuentos de solicitudes para determinar si desea bloquear las solicitudes coincidentes. Si el volumen de solicitudes sigue siendo inusualmente alto y está seguro de que sus reglas están capturando las solicitudes que están causando el alto volumen, cambie las reglas de su ACL web para bloquear las solicitudes.

3. Continúe supervisando la página de eventos para asegurarse de que su tráfico se gestiona como desee.

AWS proporciona plantillas preconfiguradas para que pueda empezar rápidamente. Las plantillas incluyen un conjunto de AWS WAF reglas que puede personalizar y utilizar para bloquear los ataques habituales basados en la web. Para obtener más información, consulte Automatizaciones de seguridad de AWS WAF.

Solicitar un crédito en AWS Shield Advanced

Si está suscrito AWS Shield Advanced y sufre un ataque DDoS que aumente la utilización de un recurso protegido de Shield Advanced, puede solicitar un crédito de servicio de Shield Advanced para los cargos relacionados con el aumento de la utilización, en la medida en que Shield Advanced no lo mitigue.

> **Note**
>
> Puede aplicar los créditos recibidos a través de este proceso solo al uso de Shield Advanced. Los créditos Shield Advanced no están disponibles para su uso con otros servicios.

Los créditos solo están disponibles para los siguientes tipos de cargos:

- Transferencia de datos Shield Advanced
- Solicitudes CloudFront HTTP/HTTPS de Amazon
- CloudFront transferencia de datos saliente
- Amazon Route 53
- AWS Global Accelerator aceleración estándar de transferencia de datos
- Unidades de capacidad del equilibrador de carga para el equilibrador de carga de aplicación
- Costos de instancias para instancias de Amazon Elastic Compute Cloud (Amazon EC2) protegidas que han sido creadas mediante una política de escalado automático en respuesta al ataque

Requisitos previos para solicitar un crédito

Para poder recibir un crédito, antes de que comenzara el ataque, debes haber hecho lo siguiente:

- Debe haber agregado la protección Shield Advanced a los recursos para los que desea solicitar un crédito. Los recursos protegidos que se añadan durante un ataque no son aptos para la protección de costos.

  > **Note**
  >
  > Al activar Shield Advanced en su Cuenta de AWS dispositivo, no se habilita automáticamente la protección de Shield Advanced para recursos individuales.

  Para obtener más información sobre cómo proteger AWS los recursos con Shield Advanced, consulteAñadir AWS Shield Advanced protección a AWS los recursos.
- Para los recursos aplicables CloudFront y protegidos por Application Load Balancer, debe haber asociado una ACL AWS WAF web e implementado una regla basada en la velocidad en la ACL web en modo. Block Para obtener información acerca de las reglas basadas en tasas de AWS WAF , consulte Instrucción de regla basada en frecuencia. Para obtener información sobre cómo asociar las ACL web con los AWS recursos, consulte. AWS WAF listas de control de acceso web (ACL web)
- Debe haber implementado las prácticas recomendadas adecuadas en Prácticas recomendadas para la resiliencia DDoS de AWS para configurar su aplicación de manera que se minimicen los costos durante un ataque DDoS.

¿Cómo solicitar un crédito?

Para poder optar a un crédito, debe presentar su solicitud de crédito dentro del período de 15 días inmediatamente siguiente al mes de facturación en el que se produjo el ataque.

Para solicitar un crédito, presente un caso de facturación a través del Centro AWS Support. En la solicitud, incluya lo siguiente:

- Las palabras «Concesión DDoS» en la línea del asunto
- Las fechas y horas de cada evento o interrupción de disponibilidad para los que solicita un crédito
- Los AWS servicios y recursos específicos que se vieron afectados

Tras enviar una solicitud, el AWS Shield Response Team (SRT) validará si se ha producido un ataque DDoS y, de ser así, si algún recurso protegido se ha escalado para absorber el ataque DDoS. Si AWS determina que los recursos protegidos se ampliaron para absorber el ataque DDoS, AWS

emitirá un crédito por la parte del tráfico que AWS determine que fue causada por el ataque DDoS. Los créditos son válidos durante 12 meses.

Seguridad en el uso del AWS Shield servicio

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

> **Note**
>
> Esta sección proporciona una guía AWS de seguridad estándar para el uso del AWS Shield servicio y sus AWS recursos, como las protecciones Shield Advanced.
> Para obtener información sobre cómo proteger sus AWS recursos con Shield and Shield Advanced, consulte el resto de la AWS Shield guía.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad que se aplican a Shield, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Shield. En los siguientes temas, se le mostrará cómo configurar Shield para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de Shield.

Temas

- Protección de datos en Shield

- Administración de identidad y acceso para AWS Shield
- Registro y supervisión en Shield
- Validación de la conformidad en Shield
- Resiliencia en Shield
- Seguridad de la infraestructura en AWS Shield

Protección de datos en Shield

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS Shield. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabajas con Shield u otro Servicios de AWS dispositivo mediante la consola, la API o AWS los SDK. AWS CLI Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Las entidades de escudo, como las protecciones, se cifran en reposo, excepto en ciertas regiones donde el cifrado no está disponible, incluidas China (Pekín) y China (Ningxia). Para cada región se utilizan claves de cifrado únicas.

Administración de identidad y acceso para AWS Shield

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Shield. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que se realice en Shield.

Usuario de servicio: si utiliza el servicio de Shield para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Shield para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica de Shield, consulte Solución de problemas AWS Shield de identidad y acceso.

Administrador de servicio: si está a cargo de los recursos de Shield en su empresa, probablemente tenga acceso completo a Shield. Su trabajo consiste en determinar a qué características y recursos de Shield deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Shield, consulte Cómo AWS Shield funciona con IAM.

Administrador de IAM: si es administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a Shield. Para consultar ejemplos de políticas basadas en identidad de Shield que puede utilizar en IAM, consulte Ejemplos de políticas basadas en identidades de AWS Shield.

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener

más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS Single Sign-On y Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS Single Sign-On. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué

pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS Single Sign-On.

- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, en algunos casos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifique el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo AWS Shield funciona con IAM

Antes de utilizar IAM para administrar el acceso a Shield, conozca qué características de IAM se pueden utilizar con Shield.

Funciones de IAM que puede utilizar con AWS Shield

Característica de IAM	Compatibilidad con Shield
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan Shield y otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas de Shield basadas en identidades

Compatibilidad con las políticas basadas en identidades	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Para ver ejemplos de políticas basadas en identidad de Shield, consulte Ejemplos de políticas basadas en identidades de AWS Shield.

Políticas basadas en recursos de Shield

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política

en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Acciones de política para Shield

Admite acciones de política	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de Shield, consulte Acciones definidas por AWS Shield en la Referencia de autorizaciones de servicio.

Las acciones de políticas de Shield utilizan el siguiente prefijo antes de la acción:

```
shield
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "shield:action1",
      "shield:action2"
         ]
```

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones de Shield que comiencen con `List`, incluya la siguiente acción:

```
"Action": "shield:List*"
```

Para ver ejemplos de políticas basadas en identidad de Shield, consulte Ejemplos de políticas basadas en identidades de AWS Shield.

Recursos de políticas de Shield

Admite recursos de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver la lista de los tipos de recursos de Shield y sus ARN, consulte Recursos definidos por AWS Shield en la Referencia de autorizaciones de servicio. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Shield. Para permitir o denegar el acceso a un subconjunto de recursos de Shield, incluya el ARN del recurso en el elemento `resource` de la política.

En AWS Shield, los recursos son protecciones y ataques. Estos recursos tienen nombres de recursos de Amazon (ARN) únicos asociados a ellos, tal y como se muestra en la siguiente tabla.

Nombre en la AWS Shield consola	Nombre en AWS Shield SDK/CLI	Formato de ARN
Evento o ataque	`AttackDetail`	`arn:aws:shield:: account:attack/ID`
Protección	`Protection`	`arn:aws:shield:: account:protection/ ID`

Para permitir o denegar el acceso a un subconjunto de recursos de Shield, incluya el ARN del recurso en el elemento `resource` de la política. Los ARN de Shield tienen el siguiente formato:

```
arn:partition:shield::account:resource/ID
```

Sustituya las variables *account*, *resource* e *ID* por valores válidos. Los valores válidos pueden ser los siguientes:

- *cuenta*: el ID de tu. Cuenta de AWS Debe especificar un valor.
- *resource*: el tipo de recurso de Shield, ya sea `attack` o `protection`.
- *ID*: el ID del recurso de Shield o un comodín (`*`) para indicar todos los recursos del tipo especificado asociados con la Cuenta de AWS en cuestión.

Por ejemplo, los siguientes ARN especifican todas las protecciones de la cuenta `111122223333`:

```
arn:aws:shield::111122223333:protection/*
```

Los ARN de los recursos de Shield tienen el siguiente formato:

```
arn:partition:shield:region:account-id:scope/resource-type/resource-name/resource-id
```

Para obtener información general acerca de las especificaciones de ARN, consulte Nombres de recursos de Amazon (ARN) en la Referencia general de Amazon Web Services.

A continuación, se enumeran los requisitos específicos de los ARN de los recursos de `wafv2`:

- *región*: En el caso de los recursos de Shield que utilizas para proteger CloudFront las distribuciones de Amazon, establécela en. `us-east-1` De lo contrario, establézcalo en la región que esté utilizando con sus recursos regionales protegidos.
- *alcance*: defina el ámbito `global` para usarlo con una CloudFront distribución de Amazon o `regional` para usarlo con cualquiera de los recursos regionales AWS WAF compatibles. Los recursos regionales son una API REST de Amazon API Gateway, un Application Load Balancer, una API AWS AppSync GraphQL, un grupo de usuarios de Amazon Cognito, un AWS App Runner servicio y una instancia de Verified Access. AWS
- *resource-type*: especifique los siguientes valores: `attack` para eventos o ataques y `protection` para protecciones.
- *resource-name*: especifique el nombre que asignó al recurso de Shield o especifique un comodín (`*`) para indicar todos los recursos que cumplen las demás especificaciones del ARN. Debe especificar el nombre y el identificador del recurso, o especificar un comodín para ambos.
- *resource-id*: especifique el ID del recurso de Shield o especifique un comodín (`*`) para indicar todos los recursos que cumplen las demás especificaciones del ARN. Debe especificar el nombre y el identificador del recurso, o especificar un comodín para ambos.

Por ejemplo, el siguiente ARN especifica todas las ACL web con ámbito regional para la cuenta `111122223333` en la región `us-west-1`:

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

El siguiente ARN especifica el grupo de reglas denominado `MyIPManagementRuleGroup` con un alcance global para la cuenta `111122223333` en la región `us-east-1`:

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

Para ver ejemplos de políticas basadas en identidad de Shield, consulte Ejemplos de políticas basadas en identidades de AWS Shield.

Claves de condición de política de Shield

Admite claves de condición de políticas específicas del servicio	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación lógica `AND`. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de Shield, consulte Claves de condición para AWS Shield en la Referencia de autorizaciones de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por AWS Shield.

Para ver ejemplos de políticas basadas en identidad de Shield, consulte Ejemplos de políticas basadas en identidades de AWS Shield.

ACL en Shield

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con Shield

Admite ABAC (etiquetas en las políticas)	Parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Shield

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes

AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para Shield

Admite Forward access sessions (FAS)	Sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio de Shield

Compatible con roles de servicio	Sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Shield. Edite los roles de servicio solo cuando Shield proporcione orientación para hacerlo.

Roles vinculados a servicios de Shield

Compatible con roles vinculados al servicio	Sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información acerca de cómo crear o administrar roles vinculados a servicios Shield, consulte Uso de roles vinculados a servicios para Shield Advanced.

Ejemplos de políticas basadas en identidades de AWS Shield

De forma predeterminada, los usuarios y roles no tienen permiso para crear o modificar recursos de Shield. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles, y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

A fin de obtener más información sobre las acciones y los tipos de recursos definidos por Shield, incluido el formato de los ARN para cada tipo de recurso, consulte Acciones, recursos y claves de condición para AWS Shield en la Referencia de autorizaciones de servicio.

Temas

- Prácticas recomendadas sobre las políticas

- Uso de la consola de Shield
- Cómo permitir a los usuarios consultar sus propios permisos
- Concesión de acceso de lectura a sus protecciones de Shield Advanced
- Otorgue acceso de solo lectura a Shield, y CloudFront CloudWatch
- Otorga acceso completo a Shield CloudFront, y CloudWatch

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Shield de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía del usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para

más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola de Shield

Para acceder a la AWS Shield consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Shield que tiene en su propiedad Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Los usuarios que pueden acceder a la AWS consola y utilizarla también pueden acceder a AWS Shield ella. No requieren otros permisos.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Concesión de acceso de lectura a sus protecciones de Shield Advanced

AWS Shield permite el acceso a los recursos entre cuentas, pero no permite crear protecciones de recursos entre cuentas. Solo puede crear protecciones para los recursos desde la cuenta que posee esos recursos.

A continuación, se muestra un ejemplo de política que concede permisos para la acción `shield:ListProtections` en todos los recursos. Shield no es compatible con la identificación de recursos concretos mediante los ARN de los recursos (también conocidos como permisos a nivel de recurso) en algunas de las acciones de la API, por lo que utilizará un comodín (*). Esto solo permite el acceso a los recursos que puede recuperar a través de la acción `ListProtections`.

```
{
    "Version": "2016-06-02",
    "Statement": [
```

```
        {
            "Sid": "ListProtections",
            "Effect": "Allow",
            "Action": [
                "shield:ListProtections"
            ],
            "Resource": "*"
        }
    ]
}
```

Otorgue acceso de solo lectura a Shield, y CloudFront CloudWatch

La siguiente política otorga a los usuarios acceso de solo lectura a Shield y a los recursos asociados, incluidos los recursos de Amazon CloudFront y las métricas de Amazon CloudWatch . Es útil para los usuarios que necesitan permiso para ver la configuración de las protecciones y los ataques de Shield y para monitorear las métricas en ella CloudWatch. Estos usuarios no pueden crear, actualizar ni eliminar recursos de Shield.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "ProtectedResourcesReadAccess",
                "Effect": "Allow",
                "Action": [
                    "cloudfront:List*",
                    "elasticloadbalancing:List*",
                    "route53:List*",
                    "cloudfront:Describe*",
                    "elasticloadbalancing:Describe*",
                    "route53:Describe*",
                    "cloudwatch:Describe*",
                    "cloudwatch:Get*",
                    "cloudwatch:List*",
                    "cloudfront:GetDistribution*",
                    "globalaccelerator:ListAccelerators",
                    "globalaccelerator:DescribeAccelerator"
                ],
                "Resource": [
                    "arn:aws:elasticloadbalancing:*:*:*",
                    "arn:aws:cloudfront::*:*",
                    "arn:aws:route53:::hostedzone/*",
```

```
                "arn:aws:cloudwatch:*:*:*:*",
                "arn:aws:globalaccelerator::*:*"
            ]
        },
        {
            "Sid": "ShieldReadOnly",
            "Effect": "Allow",
            "Action": [
                "shield:List*",
                "shield:Describe*",
                "shield:Get*"
            ],
            "Resource": "*"
        }
    ]
}
```

Otorga acceso completo a Shield CloudFront, y CloudWatch

La siguiente política permite a los usuarios realizar cualquier operación de Shield, realizar cualquier operación en distribuciones CloudFront web y monitorear las métricas y una muestra de solicitudes en CloudWatch. Resulta muy útil para los usuarios que son administradores de Shield.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "ProtectedResourcesReadAccess",
                "Effect": "Allow",
                "Action": [
                    "cloudfront:List*",
                    "elasticloadbalancing:List*",
                    "route53:List*",
                    "cloudfront:Describe*",
                    "elasticloadbalancing:Describe*",
                    "route53:Describe*",
                    "cloudwatch:Describe*",
                    "cloudwatch:Get*",
                    "cloudwatch:List*",
                    "cloudfront:GetDistribution*",
                    "globalaccelerator:ListAccelerators",
                    "globalaccelerator:DescribeAccelerator"
                ],
```

```
                "Resource": [
                    "arn:aws:elasticloadbalancing:*:*:*",
                    "arn:aws:cloudfront::*:*",
                    "arn:aws:route53:::hostedzone/*",
                    "arn:aws:cloudwatch:*:*:*:*",
                    "arn:aws:globalaccelerator::*:*"
                ]
            },
            {
                "Sid": "ShieldFullAccess",
                "Effect": "Allow",
                "Action": [
                    "shield:*"
                ],
                "Resource": "*"
            }
        ]
}
```

Recomendamos encarecidamente que configure la autenticación multifactor (MFA) para los usuarios que tienen permisos administrativos. Para obtener más información, consulte Uso de la autenticación multifactor (MFA) en dispositivos con AWS en la Guía del usuario de IAM.

AWS políticas gestionadas para AWS Shield

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSShieldDRTAccessPolicy

AWS Shield utiliza esta política gestionada cuando concedes permiso al Shield Response Team (SRT) para que actúe en tu nombre. Esta política otorga al SRT un acceso limitado a su AWS cuenta para ayudar a mitigar los ataques DDoS durante eventos de alta gravedad. Esta política permite a la SRT gestionar sus AWS WAF reglas y las protecciones de Shield Advanced y acceder a sus AWS WAF registros.

Para obtener información sobre cómo conceder permisos al SRT para que opere en su nombre, consulte. Configuración del acceso para el equipo de respuesta de Shield (SRT)

Para obtener más información sobre esta política, consulte AWSShieldDRTAccessPolicyla consola de IAM.

AWS política gestionada: AWSShieldServiceRolePolicy

Shield Advanced usa esta política administrada cuando habilita la mitigación automática de DDoS en la capa de aplicación a fin de establecer los permisos que necesita para administrar los recursos de su cuenta. Esta política permite a Shield Advanced crear y aplicar AWS WAF reglas y grupos de reglas en las ACL web que haya asociado a sus recursos protegidos para responder automáticamente a los ataques DDoS.

No puede conectarse AWSShieldServiceRolePolicy a sus entidades de IAM. Shield asocia esta política al rol vinculado a servicios `AWSServiceRoleForAWSShield` para permitir que Shield realice acciones en su nombre.

Shield Advanced permite el uso de esta política cuando se habilita la mitigación de DDoS automática en la capa de aplicación. Para obtener más información acerca del uso de esta política, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced.

Para obtener información sobre el rol vinculado al servicio AWSServiceRoleForAWSShield que usa esta política, consulte Uso de roles vinculados a servicios para Shield Advanced

Para obtener más información sobre esta política, consulte AWSShieldServiceRolePolicyen la consola de IAM.

Shield actualiza las políticas AWS gestionadas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de Shield desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de Shield en Historial de documentos.

Política	Descripción del cambio	Date
`AWSShieldServiceRolePolicy` Esta política permite a Shield acceder a AWS los recursos y gestionarlos para responder automáticamente a los ataques DDoS de la capa de aplicación en su nombre. Detalles en la consola de IAM: AWSShieldServiceRolePolicy El rol vinculado al servicio `AWSServiceRoleForAWSShield` emplea esta política. Para obtener más información, consulte Uso de roles vinculados a servicios para Shield Advanced.	Se agregó esta política para proporcionar a Shield Advanced los permisos necesarios para la funcionalidad de mitigación automática de DDoS en la capa de aplicación. Para obtener información acerca de esta característica, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced.	1 de diciembre de 2021
Shield comenzó a realizar un seguimiento de los cambios	Shield comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	3 de marzo de 2021

Solución de problemas AWS Shield de identidad y acceso

Utilice la siguiente información para ayudar a diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Shield e IAM.

Temas

No tengo autorización para realizar una acción en Shield

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `shield:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 shield:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `shield:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a Shield.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Shield. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Shield

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para obtener información acerca de si Shield admite estas características, consulte Cómo AWS Shield funciona con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Uso de roles vinculados a servicios para Shield Advanced

AWS Shield Advanced utiliza funciones vinculadas al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Shield Advanced. Shield Advanced predefine las funciones vinculadas al servicio e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio simplifica la configuración de Shield Advanced, puesto que ya no hará falta añadir manualmente los permisos necesarios. Shield Advanced define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Shield Advanced puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de Shield Advanced, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a un servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de roles vinculados a servicios para Shield Advanced

Shield Advanced usa el rol vinculado al servicio denominado. AWSServiceRoleForAWSShield Esta función permite a Shield Advanced acceder a AWS los recursos y gestionarlos para responder automáticamente a los ataques DDoS de la capa de aplicación en su nombre. Para obtener más información acerca de esta funcionalidad, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced.

El rol AWSServiceRoleForAWSShield vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `shield.amazonaws.com`

La política de permisos de roles denominada AWSShieldServiceRolePolicy permite a Shield Advanced realizar las siguientes acciones en todos los AWS recursos:

- `wafv2:GetWebACL`
- `wafv2:UpdateWebACL`
- `wafv2:GetWebACLForResource`
- `wafv2:ListResourcesForWebACL`
- `cloudfront:ListDistributions`
- `cloudfront:GetDistribution`

Cuando se permiten acciones en todos los AWS recursos, esto se indica en la política como`"Resource": "*"`. Esto solo significa que la función vinculada al servicio puede realizar cada acción indicada en todos los AWS recursos compatibles con la acción. Por ejemplo, la acción `wafv2:GetWebACL` solo es compatible con los recursos de ACL web de `wafv2`.

Shield Advanced solo realiza llamadas a la API a nivel de recursos para los recursos protegidos para los que haya habilitado la característica de protección de la capa de aplicación y para las ACL web asociadas a esos recursos protegidos.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio para Shield Advanced

No necesita crear manualmente un rol vinculado a servicios. Cuando habilita la mitigación automática de DDoS en la capa de aplicación para un recurso en la AWS Management Console AWS CLI, la o la AWS API, Shield Advanced crea automáticamente la función vinculada al servicio.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando habilita la mitigación automática de DDoS en la capa de aplicación para un recurso, Shield Advanced crea el rol vinculado al servicio para usted otra vez.

Modificación de un rol vinculado a un servicio para Shield Advanced

Shield Advanced no permite editar el rol AWSServiceRoleForAWSShield vinculado al servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM..

Eliminación de un rol vinculado a un servicio para Shield Advanced

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se monitorice ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si Shield Advanced está utilizando el rol cuando se intentan eliminar los recursos, es posible que se produzcan errores en la operación de eliminación. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de Shield Advanced que utiliza el AWSServiceRoleForAWSShield

Para todos los recursos que tengan configuradas las protecciones DDoS en la capa de aplicación, desactive la mitigación automática de DDoS de la capa de aplicación. Para obtener instrucciones sobre la consola, consulte Configure las protecciones DDoS en la capa de aplicación.

Cómo eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForAWSShield servicio. Para más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a servicios de Shield Advanced

Shield Advanced admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio esté disponible. Para obtener más información, consulte Puntos de conexiones y cuotas de Shield Advanced.

Registro y supervisión en Shield

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Shield y sus AWS soluciones. Debe recopilar los datos de supervisión de todas las partes de la AWS solución para poder depurar con mayor facilidad una falla multipunto en caso de que se produzca alguna. AWS proporciona varias herramientas para supervisar tus recursos de Shield y responder a posibles eventos:

CloudWatch Alarmas Amazon

Al usar CloudWatch las alarmas, puede observar una única métrica durante un período de tiempo que especifique. Si la métrica supera un umbral determinado, CloudWatch envía una notificación a un tema o AWS Auto Scaling política de Amazon SNS. Para obtener más información, consulte Monitorización con Amazon CloudWatch.

AWS CloudTrail Registros

CloudTrail proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Shield. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Shield, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales. Para obtener más información, consulte Registro de llamadas a la API de AWS CloudTrail con.

Validación de la conformidad en Shield

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

  > **Note**
  >
  > No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos

de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.

- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en Shield

La infraestructura AWS global se basa en distintas zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Seguridad de la infraestructura en AWS Shield

Como servicio gestionado, AWS Shield está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a Shield a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.

- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

AWS Shield Advanced cuotas

AWS Shield Advanced tiene cuotas predeterminadas en cuanto al número de entidades por región. Puede solicitar un aumento de dichas cuotas.

Recurso	Cuota predeterminada
Número máximo de recursos protegidos por cuenta para cada tipo de recurso que AWS Shield Advanced ofrece protección.	1 000
Número máximo de grupos de protección por cuenta.	100
Número máximo de recursos protegidos individuales que puede incluir específicamente en un grupo de protección. En la API, esto se aplica a los `Members` que se especifiquen al configurar el grupo de protección `Pattern` como `ARBITRARY` . En la consola, esto se aplica a los recursos que seleccione para la agrupación de protección Elija entre los recursos protegidos.	1 000

AWS Firewall Manager

AWS Firewall Manager simplifica las tareas de administración y mantenimiento en varias cuentas y recursos para una variedad de protecciones AWS WAF, AWS Shield Advanced como los grupos de seguridad de Amazon VPC y las ACL de red AWS Network Firewall, y el firewall de DNS Amazon Route 53 Resolver. Con Firewall Manager, configure las protecciones una única vez y el servicio las aplica automáticamente en todas sus cuentas y recursos, incluso cuando se agreguen nuevas cuentas y recursos.

Firewall Manager ofrece los siguientes beneficios:

- Ayuda a proteger los recursos entre cuentas
- Ayuda a proteger todos los recursos de un tipo concreto, como todas las CloudFront distribuciones de Amazon
- Ayuda a proteger todos los recursos con etiquetas específicas
- Añade automáticamente protección a los recursos que se añaden a su cuenta
- Permite suscribir todas las cuentas de los miembros de una AWS Organizations organización y suscribir AWS Shield Advanced automáticamente las nuevas cuentas dentro del ámbito que se unan a la organización
- Le permite aplicar reglas de grupo de seguridad a todas las cuentas de miembro o subconjuntos específicos de cuentas de una organización AWS Organizations y aplica de forma automática las reglas a las nuevas cuentas pertinentes que se unen a la organización.
- Te permite usar tus propias reglas o comprar reglas administradas en AWS Marketplace

Firewall Manager es especialmente útil cuando se desea proteger a toda la organización en vez de a una pequeña cantidad de cuentas y recursos específicos, o si se agregan con frecuencia nuevos recursos que se desea proteger. Firewall Manager también proporciona una supervisión centralizada de los ataques DDoS en toda la organización.

Temas

- Trabajar con AWS Firewall Manager políticas
- Trabajar con conjuntos de recursos en Firewall Manager
- Visualización de la información de cumplimiento de una AWS Firewall Manager política
- AWS Firewall Manager hallazgos
- Seguridad en el uso del AWS Firewall Manager servicio
- AWS Firewall Manager cuotas

AWS Firewall Manager precios

Los cargos en los que incurre AWS Firewall Manager son por los servicios subyacentes, como AWS WAF y AWS Config. Para obtener más información, consulte AWS Firewall Manager Precios.

AWS Firewall Manager requisitos previos

En este tema se muestra cómo prepararse para la administración. AWS Firewall Manager Utilice una cuenta de administrador de Firewall Manager para gestionar todas las políticas de seguridad de Firewall Manager de su organización en AWS Organizations. A menos que se indique lo contrario, lleve a cabo los pasos previos con la cuenta que utilizará como administrador del Firewall Manager.

Antes de usar Firewall Manager por primera vez, realice los pasos que se describen a continuación en orden.

Temas

- Paso 1: Unirse y configurar AWS Organizations
- Paso 2: Crear una cuenta de administrador AWS Firewall Manager predeterminada
- Paso 3: Habilitar AWS Config
- Paso 4: Para las políticas de terceros, suscríbase al Marketplace de AWS y configure los ajustes de terceros
- Paso 5: Para las políticas de Network Firewall y DNS Firewall, habilite el uso compartido de recursos
- Paso 6: Para usar AWS Firewall Manager en regiones que están deshabilitadas de forma predeterminada

Paso 1: Unirse y configurar AWS Organizations

Para usar Firewall Manager, su cuenta debe ser miembro de la organización del servicio de AWS Organizations en el que quiere usar sus políticas de Firewall Manager.

> **Note**
>
> Para obtener información sobre Organizaciones, consulte la Guía del usuario de AWS Organizations.

Para establecer la AWS Organizations membresía y la configuración requeridas

1. Elija una cuenta para usarla como administrador del Firewall Manager de la organización en Organizations.
2. Si la cuenta que ha elegido aún no es miembro de la organización, haga que se una. Siga las instrucciones que se indican en Invitar Cuenta de AWS a un hombre a unirse a su organización.
3. AWS Organizations tiene dos conjuntos de funciones disponibles: funciones de facturación unificada y todas las funciones. Para utilizar Firewall Manager, la organización debe estar habilitada para todas las características. Si su organización está configurada solo para la facturación unificada, consulte la guía Habilitación de todas las características en la organización.

Paso 2: Crear una cuenta de administrador AWS Firewall Manager predeterminada

Este procedimiento utiliza la cuenta y la organización que eligió y configuró en el paso anterior.

Solo la cuenta de administración de la organización puede crear cuentas de administrador predeterminadas del Firewall Manager. La primera cuenta de administrador que cree es la cuenta de administrador predeterminada. La cuenta de administrador predeterminada puede administrar firewalls de terceros y tiene un alcance administrativo completo. Al configurar la cuenta de administrador predeterminada, el Administrador de Firewall la establece automáticamente como administrador AWS Organizations delegado de Firewall Manager. Esto permite a Firewall Manager acceder a la información sobre las unidades organizativas (UO) de la organización. Puede utilizar las unidades organizativas para especificar el alcance de las políticas de Firewall Manager. Para obtener

más información sobre cómo establecer el alcance de la política, consulte las instrucciones para los tipos de políticas individuales que aparecen en Creación de una AWS Firewall Manager política. Para obtener más información sobre Organizations y las cuentas de administración, consulte Administrar las AWS cuentas de su organización.

Configuración necesaria para la cuenta de administración de la organización

La cuenta de administración de la organización debe tener la siguiente configuración para poder incorporar la organización al Firewall Manager y crear un administrador predeterminado:

- Debe ser miembro de la organización en la AWS Organizations que desee aplicar las políticas de Firewall Manager.

Cambiar la cuenta de administrador predeterminada

1. Inicie sesión en el Firewall Manager AWS Management Console con una cuenta AWS Organizations de administración existente.
2. Abra la consola de Firewall Manager en https://console.aws.amazon.com/wafv2/fmsv2.
3. En el panel de navegación, seleccione Configuración.
4. Escriba el ID de AWS cuenta de la cuenta que ha elegido usar como administrador del Firewall Manager.

   > **Note**
   >
   > El administrador predeterminado tiene todo el ámbito administrativo. El ámbito administrativo completo significa que esta cuenta puede aplicar políticas a todas las cuentas y unidades organizativas (UO) de la organización, tomar medidas en todas las regiones y administrar todos los tipos de políticas de Firewall Manager.

5. Seleccione Crear cuenta de administrador para crear la cuenta.

Para obtener más información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte Trabajar con AWS Firewall Manager los administradores.

Paso 3: Habilitar AWS Config

Para usar Firewall Manager, debe habilitar AWS Config.

> **Note**
>
> Se le cobrará por su AWS Config configuración, según el AWS Config precio. Para obtener más información, consulta Cómo empezar con AWS Config.

> **Note**
>
> Para que Firewall Manager supervise el cumplimiento de las políticas, AWS Config debe registrar continuamente los cambios de configuración de los recursos protegidos. En su AWS Config configuración, la frecuencia de grabación debe estar establecida en Continua, que es la configuración predeterminada.

AWS Config Para activar Firewall Manager

1. AWS Config Actívela para cada una de sus cuentas de AWS Organizations miembro, incluida la cuenta de administrador del Firewall Manager. Para obtener más información, consulte Cómo empezar con AWS Config.
2. AWS Config Actívela para cada una de las Región de AWS que contengan los recursos que desee proteger. Puede habilitarlo AWS Config manualmente o puede usar la AWS CloudFormation plantilla «Habilitar AWS Config» en Plantillas AWS CloudFormation StackSets de muestra.

   Si no desea habilitarla AWS Config para todos los recursos, debe habilitar lo siguiente según el tipo de políticas de Firewall Manager que utilice:

   - Política de WAF: habilite Config para los tipos de recursos CloudFront Distribution, Application Load Balancer (ElasticLoadBalancingelija V2 de la lista), API Gateway, WAF WebACL, WAF Regional WebACL y WAFv2 WebACL. AWS Config Para poder proteger una CloudFront distribución, debe estar en la región EE.UU. Este (Norte de Virginia). Otras regiones no tienen CloudFront esta opción.
   - Política de protección: habilite Config para los tipos de recursos Shield Protection, ShieldRegional Protection, Application Load Balancer, EC2 EIP, WAF WebACL, WAF Regional WebACL y WAFv2 WebACL.
   - Política de grupo de seguridad: habilite Config para los tipos de recursos EC2 SecurityGroup, EC2 Instance y EC2. NetworkInterface

- Política de ACL de red: habilite Config para los tipos de recursos Amazon EC2 Subnet y Amazon EC2 Network ACL.
- Política de Network Firewall: habilite Config para los tipos de recursos NetworkFirewall FirewallPolicy NetworkFirewallRuleGroup, VPC de EC2, EC2, InternetGateway EC2 y subred de RouteTable EC2.
- Política de firewall de DNS: habilite Config para el tipo de recurso EC2 VPC.
- Política de firewall de terceros: habilite Config para los tipos de recursos Amazon EC2 VPC, Amazon EC2, Amazon EC2, InternetGateway Amazon EC2 Subnet y Amazon EC2 RouteTable VPCendpoint.

> **Note**
>
> Si configura su AWS Config grabadora para usar una función de IAM personalizada, debe asegurarse de que la política de IAM tenga los permisos adecuados para registrar los tipos de recursos necesarios de la política de Firewall Manager. Sin los permisos adecuados, es posible que no se registren los recursos necesarios, lo que impide que Firewall Manager proteja sus recursos de la manera correcta. Firewall Manager no puede ver estos errores de configuración de permisos. Para obtener información sobre el uso de IAM con AWS Config, consulte IAM for. AWS Config

Paso 4: Para las políticas de terceros, suscríbase al Marketplace de AWS y configure los ajustes de terceros

Complete los siguientes requisitos previos para empezar a utilizar las políticas de firewall de terceros de Firewall Manager.

Requisitos previos de la política de firewall nativo en la nube (CNF) de Fortigate como servicio

Uso de Fortigate CNF para Firewall Manager

1. Suscríbase al Firewall nativo de la nube (CNF) de Fortigate como servicio en Marketplace AWS .
2. En primer lugar, registre un inquilino en el portal de productos CNF de Fortigate. A continuación, añada su cuenta de administrador de Firewall Manager a su inquilino en el portal de productos CNF de Fortigate. Para obtener más información, consulte la Documentación de Fortigate CNF.

Si necesita más información sobre el trabajo con las políticas de Fortigate CNF, consulte Políticas de Fortigate Cloud Native Firewall (CNF) como servicio.

Requisitos previos de la política de firewall de próxima generación de Palo Alto Networks Cloud

Uso de Palo Alto Networks Cloud NGFW para Firewall Manager

1. Suscríbase al servicio Pay-As-You-Go de próxima generación de firewall en la nube de Palo Alto Networks en Marketplace. AWS
2. Complete los pasos de despliegue del NGFW en la nube de Palo Alto Networks que se indican en la guía Implemente el NGFW en la nube de Palo Alto Networks para continuar AWS con el AWS Firewall Manager tema de la guía de implementación del firewall de próxima generación en la nube de Palo Alto Networks. AWS

Para obtener información sobre el uso de las políticas de NGFW de Palo Alto Networks en la nube, consulte Políticas de NGFW en la nube de Palo Alto Networks.

Paso 5: Para las políticas de Network Firewall y DNS Firewall, habilite el uso compartido de recursos

Para administrar las políticas de Firewall Manager, Network Firewall y DNS Firewall, debe habilitar el uso compartido con AWS Organizations in AWS Resource Access Manager. Esto permite que Firewall Manager implemente protecciones en sus cuentas cuando cree estos tipos de políticas.

Para habilitar el uso compartido AWS Organizations con AWS Resource Access Manager

- Siga las instrucciones de Habilitación del uso compartido con AWS Organizations en la Guía del usuario de AWS Resource Access Manager .

Si tiene problemas con el uso compartido de recursos, consulte las instrucciones en Uso compartido de recursos para las políticas de Network Firewall y DNS Firewall.

Paso 6: Para usar AWS Firewall Manager en regiones que están deshabilitadas de forma predeterminada

Para usar el Administrador de Firewall en una región que está deshabilitada de forma predeterminada, debe habilitar la Región tanto para la cuenta de administración de su AWS

organización como para la cuenta de administrador predeterminada del Firewall Manager. Para obtener información sobre las regiones que están deshabilitadas de forma predeterminada y cómo habilitarlas, consulte Administración de Regiones de AWS en la Referencia general de AWS .

Habilitación de una región deshabilitada

- Tanto para la cuenta de administración de Organizaciones como para la cuenta de administrador predeterminada de Firewall Manager, siga las instrucciones de Habilitación de una región en la Referencia general de AWS .

Después de seguir estos pasos, puede configurar Firewall Manager para empezar a proteger sus recursos. Para obtener más información, consulte Cómo empezar con AWS Firewall ManagerAWS WAF las políticas.

Trabajar con AWS Firewall Manager los administradores

Con AWS Firewall Manager él puede tener uno o varios administradores que puedan administrar los recursos de firewall de su organización. Si desea utilizar varios administradores de Firewall Manager en su organización, puede aplicar condiciones de ámbito administrativo a cada administrador para definir los recursos que pueden administrar. Esto le da la flexibilidad de tener diferentes funciones de administrador en su organización y le ayuda a mantener el principio de acceso con privilegio mínimo. Por ejemplo, puede hacer que un administrador administre un conjunto de unidades organizativas (UO) para su organización y delegar a otro administrador la tarea de administrar solo tipos de políticas específicos de Firewall Manager. Para obtener más información sobre Organizations y las cuentas de administración, consulte Administrar las AWS cuentas de su organización.

Para ver el número máximo de administradores que puede tener por organización, consulte AWS Firewall Manager cuotas.

Introducción al uso de administradores de Firewall Manager

Antes de comenzar a usar administradores de Firewall Manager, debe completar los requisitos previos que se enumeran en AWS Firewall Manager requisitos previos. Según los requisitos previos, incorporará una AWS Organizations organización a Firewall Manager y creará una cuenta de administrador predeterminada para Firewall Manager. Una cuenta de administrador predeterminada tiene la capacidad de administrar firewalls de terceros y tiene un ámbito administrativo completo.

Ámbito administrativo

El ámbito administrativo define los recursos que el administrador de Firewall Manager puede administrar. Después de que una cuenta de AWS Organizations administración incorpore una organización a Firewall Manager, la cuenta de administración puede crear administradores de Firewall Manager adicionales con diferentes ámbitos administrativos. Una cuenta AWS Organizations de administración puede conceder al administrador un ámbito administrativo completo o restringido. El ámbito completo proporciona al administrador acceso total a todos los tipos de recursos anteriores. El ámbito restringido se refiere a la concesión de permisos administrativos únicamente a un subconjunto de los recursos anteriores. Se recomienda conceder únicamente a los administradores los permisos que necesitan para realizar las tareas propias de su función. Puede aplicar cualquier combinación de estas condiciones de ámbito administrativo a un administrador:

- Cuentas o unidades organizativas de su organización a las que el administrador puede aplicar políticas.
- Regiones en las que el administrador puede realizar acciones.
- Tipos de políticas de Firewall Manager que el administrador puede administrar.

Funciones de administrador

Hay dos tipos de funciones de administrador en Firewall Manager: administrador predeterminado y administradores de Firewall Manager.

- Administrador predeterminado: la cuenta de administración de la organización crea una cuenta de administrador predeterminado de Firewall Manager al incorporar su organización a Firewall Manager mientras completa la AWS Firewall Manager requisitos previos. El administrador predeterminado puede administrar firewalls de terceros y tiene un ámbito administrativo completo, pero, por lo demás, está al mismo nivel que los demás administradores, en caso de que decida tener varios.
- Administradores de Firewall Manager: un administrador de Firewall Manager puede administrar los recursos que la cuenta de administración de AWS Organizations le designa en la configuración de su ámbito administrativo. Para ver el número máximo de administradores que puede tener por organización, consulte AWS Firewall Manager cuotas. Al crear una cuenta de administrador de Firewall Manager, el servicio comprueba si la cuenta ya es un administrador delegado de Firewall Manager dentro de la organización. AWS Organizations Si no es así, Firewall Manager llama a Organizations para configurar la cuenta como administrador delegado de Firewall Manager. Para obtener información sobre los administradores delegados de Organizations, consulte Terminología y conceptos de AWS Organizations en la Guía del usuario de AWS Organizations .

Administradores existentes

Si ya es cliente de Firewall Manager y ya ha establecido un administrador, este administrador existente será el administrador predeterminado de Firewall Manager. Su flujo actual no debería verse afectado. Si desea agregar más administradores, puede hacerlo siguiendo los procedimientos de este capítulo.

Creación, actualización y revocación de cuentas de administrador de Firewall Manager

Los procedimientos de los siguientes temas explican cómo crear, actualizar y revocar cuentas de administrador de Firewall Manager. Solo la cuenta de administración de una organización puede crear y actualizar las cuentas de administrador de Firewall Manager. Solo un administrador individual de Firewall Manager puede revocar su propia cuenta de administrador.

Creación de una cuenta de administrador de Firewall Manager

El siguiente procedimiento describe cómo crear cuentas de administrador de Firewall Manager con la consola de Firewall Manager.

Creación de una cuenta de administrador de Firewall Manager

1. Inicie sesión en el Firewall Manager AWS Management Console con una cuenta AWS Organizations de administración existente.
2. Abra la consola de Firewall Manager en https://console.aws.amazon.com/wafv2/fmsv2.
3. En el panel de navegación, seleccione Configuración.
4. Seleccione Crear cuenta de administrador.
5. En el panel Detalles, en el ID de cuenta de AWS , escriba el ID de AWS de la cuenta miembro que desee agregar como administrador de Firewall Manager.
6. En Ámbito administrativo, elija una de las siguientes opciones:

   - Completo: esto otorga al administrador la capacidad de aplicar políticas a todas las cuentas y unidades organizativas (UO) de la organización, tomar medidas en todas las regiones y aplicar todos los tipos de políticas de Firewall Manager, excepto los firewalls de terceros. Solo el administrador predeterminado puede crear y administrar firewalls de terceros. Tenga cuidado al conceder este nivel de permisos al administrador. En aras del privilegio mínimo, recomendamos conceder al administrador únicamente los permisos que necesite para desempeñar las funciones propias de su puesto.

- Restringido: si se aplicado un ámbito Restringido, configure las cuentas y unidades organizativas, las regiones y los tipos de políticas que la cuenta puede gestionar en Configurar el ámbito administrativo.

  Para Cuentas y unidades organizativas, elija las siguientes opciones:

  - Si quieres aplicar políticas a todas las cuentas o unidades organizativas de tu organización, selecciona Incluir todas las cuentas de mi AWS organización.
  - Si quieres aplicar las políticas solo a cuentas específicas o a cuentas que se encuentran en unidades AWS Organizations organizativas (OU) específicas, selecciona Incluir solo las cuentas y unidades organizativas especificadas y, a continuación, agrega las cuentas y unidades organizativas que desees incluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.
  - Si desea aplicar políticas a todas las cuentas o unidades AWS Organizations organizativas (OU) excepto a un conjunto específico, elija Excluir las cuentas y unidades organizativas especificadas e incluir todas las demás y, a continuación, agregue las cuentas y unidades organizativas que desee excluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.

  En Regiones, seleccione una de las siguientes opciones:

  - Si quiere permitir que el administrador realice acciones en todas las regiones disponibles, seleccione Incluir todas las regiones.
  - Si desea que el administrador realice acciones solo en regiones específicas, elija Incluir solo las regiones especificadas y, a continuación, especifique las regiones que desea incluir.

  > **Note**
  >
  > Para incluir una región que está deshabilitada de forma predeterminada, debe habilitar la región tanto para la cuenta de administración de la AWS Organizations organización como para la cuenta de administración predeterminada. Para obtener información sobre cómo habilitar regiones en una cuenta, consulte Habilitación de una región en Referencia general de Amazon Web Services.

En Tipos de políticas, elija las siguientes opciones:

- Si desea permitir que el administrador administre todos los tipos de políticas, elija Incluir todos los tipos de políticas.
- Si desea que el administrador administre solo tipos de políticas específicos, elija Incluir solo los tipos de políticas especificados y, a continuación, especifique los tipos de políticas que desea incluir.

7. Seleccione Crear cuenta de administrador para crear la cuenta de administrador. Tras la creación, el Firewall Manager llama AWS Organizations para comprobar si el administrador ya es administrador delegado de su organización. De lo contrario, Firewall Manager designará la cuenta como administrador delegado. Para obtener información sobre administradores delegados en Organizations, consulte Terminología y conceptos de AWS Organizations en la Guía del usuario de AWS Organizations .

Si aplica un ámbito administrativo restringido, Firewall Manager evalúa automáticamente cualquier recurso nuevo en función de su configuración. Por ejemplo, si solo incluye cuentas específicas, Firewall Manager no aplica la política a ninguna cuenta nueva. Como otro ejemplo, si incluye una unidad organizativa, cuando agrega una cuenta a la unidad organizativa o a cualquiera de sus unidades organizativas secundarias, Firewall Manager incluye automáticamente la cuenta en el ámbito administrativo.

Actualización de una cuenta de administrador de Firewall Manager

El siguiente procedimiento describe cómo actualizar cuentas de administrador de Firewall Manager con la consola de Firewall Manager.

> **Note**
>
> Para actualizar el ámbito de un administrador para incluir una región que está deshabilitada de forma predeterminada, debes habilitar la región tanto para la cuenta de administración de la AWS Organizations organización como para la cuenta de administración predeterminada. Para obtener información sobre cómo habilitar regiones en una cuenta, consulte Habilitación de una región en Referencia general de Amazon Web Services.

Para actualizar una cuenta de administrador (consola)

1. Inicie sesión en el Firewall Manager AWS Management Console con una cuenta AWS Organizations de administración existente.
2. Abra la consola de Firewall Manager en https://console.aws.amazon.com/wafv2/fmsv2.
3. En el panel de navegación, seleccione Configuración.
4. En la tabla Administradores de Firewall Manager, elija la cuenta que desee actualizar.
5. Seleccione Editar para cambiar los detalles de la cuenta del administrador. No se puede cambiar el ID de la cuenta.
6. Elija Guardar para guardar los cambios.

Revocación de una cuenta de administrador

El siguiente procedimiento describe cómo revocar una cuenta de administrador de Firewall Manager. Si es el administrador predeterminado, antes de poder revocar su cuenta, todas las cuentas de administrador de Firewall Manager de su organización deben revocar sus propias cuentas en primer lugar. Cómo revocar una cuenta de administrador, siga el procedimiento a continuación

Cómo revocar una cuenta de administrador (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.
2. En el panel de navegación, seleccione Configuración.
3. En el panel de Cuentas de administrador, seleccione Revocar cuenta de administrador para revocar su cuenta.

> **Important**
>
> Si revoca los privilegios de administrador de la cuenta de una cuenta de administrador, se eliminarán todas las políticas de Firewall Manager creadas mediante dicha cuenta.

Cambio de la cuenta de administrador predeterminada

Solo puede designar una cuenta en una organización como cuenta de administrador predeterminada de Firewall Manager. La cuenta de administrador predeterminada sigue el principio de “primero en entrar, último en salir”. Para designar una cuenta de administrador predeterminada diferente, cada cuenta de administrador individual debe revocar su propia cuenta en primer lugar. A continuación, el administrador predeterminado existente puede revocar su propia cuenta, lo que también excluirá a la organización de Firewall Manager. Cuando un administrador revoque su cuenta, se eliminarán todas las políticas de Firewall Manager creadas mediante dicha cuenta. Para designar una nueva cuenta de administrador predeterminada, debe iniciar sesión en Firewall Manager con la cuenta AWS Organizations de administración para designar una nueva cuenta de administrador. Para cambiar la cuenta de administrador predeterminada de una organización, realice el siguiente procedimiento.

Cómo cambiar la cuenta de administrador predeterminada

1. Inicie sesión en el Firewall Manager AWS Management Console con una cuenta AWS Organizations de administración existente.
2. Abra la consola de Firewall Manager en https://console.aws.amazon.com/wafv2/fmsv2.
3. En el panel de navegación, seleccione Configuración.
4. Escriba el ID de la cuenta que ha elegido usar como administrador de Firewall Manager.

> **Note**
>
> A la cuenta se le concede permiso para crear y administrar políticas de Firewall Manager en todas las cuentas dentro de la organización.

5. Seleccione Crear cuenta de administrador.
6. Escriba el AWS ID de la cuenta que ha elegido usar como administrador del Firewall Manager.

> **Note**
>
> A esta cuenta se le otorga un ámbito administrativo completo. El ámbito administrativo completo significa que esta cuenta puede aplicar políticas a todas las cuentas y unidades organizativas (UO) de la organización, tomar medidas en todas las regiones y administrar todos los tipos de políticas de Firewall Manager.

7. Seleccione Crear cuenta de administrador para crear la cuenta de administrador predeterminada.

Cambios inhabilitantes en una cuenta de administrador

Algunos cambios en una cuenta de administrador pueden inhabilitarla como cuenta de administrador.

En esta sección se describen los cambios que pueden inhabilitar una cuenta de administrador AWS y cómo gestiona estos cambios el Firewall Manager.

Cuenta eliminada de la organización en AWS Organizations

Si la cuenta de AWS Firewall Manager administrador se elimina de la organización en AWS Organizations, ya no podrá administrar las políticas de la organización. Firewall Manager realiza una de las siguientes acciones:

- Cuenta sin políticas: si la cuenta de administrador de Firewall Manager no tiene políticas de Firewall Manager, Firewall Manager revoca la cuenta de administrador.
- Cuenta con políticas de Firewall Manager: si la cuenta de administrador del Firewall Manager tiene políticas de Firewall Manager, Firewall Manager le envía un correo electrónico para informarle de la situación y proporcionarle las opciones que puede elegir, con la ayuda de su representante de cuentas de AWS ventas.

Cuenta cerrada

Si cierra la cuenta que está utilizando como AWS Firewall Manager administrador AWS y Firewall Manager, gestione el cierre de la siguiente manera:

- AWS revoca el acceso de administrador de la cuenta desde el Firewall Manager y el Firewall Manager desactiva todas las políticas administradas por la cuenta de administrador. Las protecciones que proporcionaban dichas políticas se detienen en toda la organización.
- AWS conserva los datos de la política del Firewall Manager de la cuenta durante 90 días a partir de la fecha de entrada en vigor del cierre de la cuenta del administrador. Durante dicho período de 90 días, puede volver a abrir la cuenta cerrada.
  - Si vuelve a abrir la cuenta cerrada durante el período de 90 días, la AWS reasigna como administrador del Firewall Manager y recupera los datos de la política del Firewall Manager de la cuenta.

- De lo contrario, al final del período de 90 días, eliminará AWS permanentemente todos los datos de política del Firewall Manager de la cuenta.

Cómo empezar con AWS Firewall Manager las políticas

Puede utilizarlas AWS Firewall Manager para habilitar varios tipos diferentes de políticas de seguridad. Los pasos de configuración difieren ligeramente en cada caso.

Temas

Cómo empezar con AWS Firewall ManagerAWS WAF las políticas

AWS Firewall Manager Para habilitar AWS WAF las reglas en toda su organización, lleve a cabo los siguientes pasos en secuencia.

Temas

Paso 1: completar los requisitos previos

Existen varios pasos obligatorios para preparar su cuenta de AWS Firewall Manager. Estos pasos se describen en AWS Firewall Manager requisitos previos. Complete todos los requisitos previos antes de continuar con Paso 2: Crear y aplicar una AWS WAF política.

Paso 2: Crear y aplicar una AWS WAF política

Una AWS WAF política de Firewall Manager contiene los grupos de reglas que desea aplicar a sus recursos. Firewall Manager crea una ACL web de Firewall Manager en cada cuenta en la que se aplica la política. Los administradores de cuentas individuales pueden agregar reglas y grupos de reglas a la ACL web resultante, además de los grupos de reglas que defina aquí. Para obtener información sobre AWS WAF las políticas de Firewall Manager, consulteAWS WAF políticas.

Para crear una AWS WAF política de Firewall Manager (consola)

Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

1. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
2. Elija Crear política.
3. Para Policy type (Tipo de política), seleccione AWS WAF.
4. En Región, elija una Región de AWS. Para proteger CloudFront las distribuciones de Amazon, elige Global.

   Para proteger los recursos en varias regiones (distintas de CloudFront las distribuciones), debe crear políticas de Firewall Manager independientes para cada región.
5. Elija Siguiente.
6. En Nombre de política, introduzca un nombre descriptivo. Firewall Manager incluye el nombre de la política en los nombres de las ACL web que administra. Los nombres de las ACL web `FMManagedWebACLV2-` van seguidos del nombre de la política que se introduce aquí, `-`, y de la marca temporal de creación de las ACL web, en milisegundos UTC. Por ejemplo, `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`.

   > **Important**
   >
   > Los nombres de las ACL web no pueden cambiarse después de la creación. Si actualiza el nombre de su política, Firewall Manager no actualizará el nombre de la ACL web asociada. Para que Firewall Manager cree una ACL web con un nombre diferente, debe crear una política nueva.

7. En Policy rules (Reglas de política), para First rule groups (Primeros grupos de reglas), elija Add rule groups (Agregar grupos de reglas). Expanda los grupos de reglas de administrados de AWS . En Core rule set (Conjunto de reglas principales), active la opción Add to web ACL (Agregar a la ACL web). En entradas incorrectas conocidas de AWS , active Agregar a la ACL web. Elija Add rules (Agregar reglas).

   En Last rule groups (Últimos grupos de reglas), elija Add rule groups (Agregar grupos de reglas). Expanda los grupos de reglas administradas de AWS y en lista de reputación de IP de Amazon, active la opción Agregar a la ACL web. Elija Add rules (Agregar reglas).

   En Primeros grupos de reglas, seleccione Conjunto de reglas básicas y elija Bajar. AWS WAF evalúa las solicitudes web comparándolas con el grupo de reglas de entradas incorrectas AWS conocidas antes de compararlas con el conjunto de reglas básicas.

   Si lo desea, también puede crear sus propios grupos de AWS WAF reglas mediante la AWS WAF consola. Los grupos de reglas que cree aparecen en Your rule groups (Sus grupos de reglas) en la página Describe policy: Add rule groups (Describir política: agregar grupos de reglas).

   El primer y el último grupo de AWS WAF reglas que administra a través del Firewall Manager tienen nombres que comienzan con `PREFMManaged-` o`POSTFMManaged-`, respectivamente, seguidos del nombre de la política del Administrador de Firewall y la marca de tiempo de creación del grupo de reglas, en milisegundos UTC. Por ejemplo, `PREFMManaged-MyWAFPolicyName-1621880555123`.
8. Deje la acción predeterminada para la ACL web en Allow (Permitir).
9. Deje la opción Policy action (Acción de política) en el valor predeterminado, para que no se corrijan automáticamente los recursos no conformes. Puede cambiar la opción más adelante.
10. Elija Siguiente.
11. En Policy scope (Enfoque de la política), proporcione la configuración de las cuentas, tipos de recursos y etiquetado que identifican los recursos a los que desea aplicar la política. Para este tutorial, deje los valores de Cuentas de AWS y Recursos y elija uno o más tipos de recursos.
12. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.

13. Elija Siguiente.
14. En el caso de las etiquetas de política, añada las etiquetas de identificación que desee añadir al recurso de políticas del Firewall Manager. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.
15. Elija Siguiente.
16. Revise la nueva configuración de la política y vuelva a las páginas en las que necesite realizar algún ajuste.

    Compruebe que Acciones de la política está establecido en Identificar los recursos que no cumplan las reglas de la política, pero sin corregirlos automáticamente. Esto te permite revisar los cambios que introduciría tu política antes de activarlos.
17. Cuando esté satisfecho con la política, elija Crear política.

    En el panel de políticas de AWS Firewall Manager , su política debe aparecer en la lista. Probablemente indique Pendiente en los encabezados de cuentas e indique el estado de la configuración de corrección automática. La creación de una política puede tardar varios minutos. Después de reemplazar el estado Pending (Pendiente) por recuentos de cuentas, puede elegir el nombre de la política para explorar el estado de cumplimiento de las cuentas y los recursos. Para obtener información, consulte Visualización de la información de cumplimiento de una AWS Firewall Manager política

Paso 3: Eliminación

Para evitar cargos imprevistos, elimine las políticas y los recursos innecesarios.

Para eliminar una política (consola)

1. En la página Políticas de AWS Firewall Manager , elija el botón de opción situado junto al nombre de la política y, a continuación, elija Eliminar.

2. En el cuadro de confirmación Delete (Eliminar), seleccione Delete all policy resources (Eliminar todos los recursos de política) y, a continuación, elija Delete (Eliminar) de nuevo.

   AWS WAF elimina la política y todos los recursos asociados, como las ACL web, que haya creado en tu cuenta. Los cambios pueden tardar unos minutos en propagarse a todas las cuentas.

Cómo empezar con AWS Firewall ManagerAWS Shield Advanced las políticas

Puede utilizarlas AWS Firewall Manager para habilitar AWS Shield Advanced las protecciones en toda su organización.

> **Important**
>
> Firewall Manager no es compatible con Amazon Route 53 o AWS Global Accelerator. Si necesita proteger estos recursos con Shield Advanced, no puede utilizar una política de Firewall Manager. En su lugar, siga las instrucciones en Añadir AWS Shield Advanced protección a AWS los recursos.

Para utilizar Firewall Manager para habilitar la protección de Shield Advanced, siga los siguientes pasos por orden.

Temas

- Paso 1: completar los requisitos previos
- Paso 2: Crear y aplicar una política de Shield Advanced
- Paso 3: (opcional) Autorizar al Equipo de Respuesta de Shield (SRT)
- Paso 4: Configurar las notificaciones de Amazon SNS y las alarmas de Amazon CloudWatch

Paso 1: completar los requisitos previos

Existen varios pasos obligatorios para preparar su cuenta de AWS Firewall Manager. Estos pasos se describen en AWS Firewall Manager requisitos previos. Complete todos los requisitos previos antes de continuar con Paso 2: Crear y aplicar una política de Shield Advanced.

Paso 2: Crear y aplicar una política de Shield Advanced

Tras cumplir los requisitos previos, se crea una política de AWS Firewall Manager Shield Advanced. Una política de Firewall Manager Shield Advanced contiene las cuentas y los recursos que desea proteger con Shield Advanced.

> **Important**
>
> Firewall Manager no es compatible con Amazon Route 53 o AWS Global Accelerator. Si necesita proteger estos recursos con Shield Advanced, no puede utilizar una política de Firewall Manager. En su lugar, siga las instrucciones en Añadir AWS Shield Advanced protección a AWS los recursos.

Creación de una política de Firewall Manager para Shield Advanced (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Elija Crear política.
4. Para el tipo de política, seleccione Shield Advanced.

   Para crear una política de Shield Advanced, su cuenta de administrador de Firewall Manager debe estar suscrita a Shield Advanced. Se le pedirá que se suscriba si no lo ha hecho ya. Para obtener más información sobre el costo de suscripción, consulte Precios de AWS Shield Advanced.

> **Note**
>
> No es necesario suscribir manualmente cada cuenta de miembro a Shield Advanced. Firewall Manager lo hace por usted cuando crea la política. Cada cuenta debe permanecer suscrita a Firewall Manager y Shield Advanced para seguir protegiendo los recursos de la cuenta.

5. En Región, elija una Región de AWS. Para proteger CloudFront los recursos de Amazon, elige Global.

   Para proteger los recursos de varias regiones (distintas de CloudFront los recursos), debe crear políticas de Firewall Manager independientes para cada región.
6. Elija Siguiente.
7. En Nombre, introduzca un nombre descriptivo.
8. (Solo para la región global) Para las políticas de la región global, puede elegir si desea gestionar la mitigación automática de DDoS en la capa de aplicaciones de Shield Advanced. Para este tutorial, deje esta opción con la configuración predeterminada de Ignorar.
9. Para la Acción de la política, elija la opción que no corrija automáticamente.
10. Elija Siguiente.
11. Cuentas de AWS Esta política se aplica para permitirle limitar el alcance de su política especificando las cuentas que desea incluir o excluir. En este tutorial, elija Include all accounts under my organization (Incluir todas las cuentas de mi organización).
12. Escoja los tipos de recursos que desea proteger.

    Firewall Manager no es compatible con Amazon Route 53 o AWS Global Accelerator. Si necesita proteger estos recursos con Shield Advanced, no puede utilizar una política de Firewall Manager. En su lugar, siga las instrucciones de Shield Advanced en Añadir AWS Shield Advanced protección a AWS los recursos.
13. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

    Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.

14. Elija Siguiente.
15. En el caso de las etiquetas de política, añada las etiquetas de identificación que desee añadir al recurso de políticas del Firewall Manager. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.
16. Elija Siguiente.
17. Revise la nueva configuración de la política y vuelva a las páginas en las que necesite realizar algún ajuste.

    Compruebe que Acciones de la política está establecido en Identificar los recursos que no cumplan las reglas de la política, pero sin corregirlos automáticamente. Esto te permite revisar los cambios que introduciría tu política antes de activarlos.
18. Cuando esté satisfecho con la política, elija Crear política.

    En el panel de políticas de AWS Firewall Manager , su política debe aparecer en la lista. Probablemente indique Pendiente en los encabezados de cuentas e indique el estado de la configuración de corrección automática. La creación de una política puede tardar varios minutos. Después de reemplazar el estado Pending (Pendiente) por recuentos de cuentas, puede elegir el nombre de la política para explorar el estado de cumplimiento de las cuentas y los recursos. Para obtener información, consulte Visualización de la información de cumplimiento de una AWS Firewall Manager política

Siga en Paso 3: (opcional) Autorizar al Equipo de Respuesta de Shield (SRT).

Paso 3: (opcional) Autorizar al Equipo de Respuesta de Shield (SRT)

Una de las ventajas AWS Shield Advanced es el apoyo del Shield Response Team (SRT). Cuando se produce un posible ataque de DDoS, puede ponerse en contacto con el Centro de AWS Support. Si es necesario, el Centro de soporte remite su problema al SRT. El SRT ayuda a analizar la actividad sospechosa y a mitigar el problema. Esta mitigación suele implicar la creación o actualización de AWS WAF reglas y ACL web en su cuenta. El SRT puede inspeccionar tu AWS WAF configuración y crear o actualizar AWS WAF reglas y ACL web por ti, pero el equipo necesita tu autorización para hacerlo. Le recomendamos que, como parte de la configuración AWS Shield Advanced, proporcione al SRT de forma proactiva la autorización necesaria. Dar permiso

de antemano ayudará a evitar retrasos en la mitigación en caso de que se produzca un verdadero ataque.

Debe autorizar y contactar con el SRT en el nivel de cuenta. Le informamos que, el propietario de la cuenta, no el administrador de Firewall Manager, debe seguir los siguientes pasos para autorizar al SRT a mitigar posibles ataques. El administrador de Firewall Manager puede autorizar al SRT solo para las cuentas de las que sean propietarios. Del mismo modo, solo el propietario de la cuenta puede ponerse en contacto con el SRT para obtener soporte.

> **Note**
>
> Para utilizar los servicios del SRT, debe haberse registrado en el plan Business Support o en el plan Enterprise Support.

Para autorizar al SRT a mitigar en su nombre los posibles ataques, siga las instrucciones en Asistencia del equipo de respuesta de Shield (Shield Response Team, SRT). Puede cambiar el acceso y los permisos del SRT en cualquier momento siguiendo los mismos pasos.

Siga en Paso 4: Configurar las notificaciones de Amazon SNS y las alarmas de Amazon CloudWatch .

Paso 4: Configurar las notificaciones de Amazon SNS y las alarmas de Amazon CloudWatch

Puede continuar con este paso sin configurar las notificaciones o CloudWatch alarmas de Amazon SNS. Sin embargo, la configuración de estas alarmas y notificaciones aumenta considerablemente su visibilidad de los posibles eventos de DDoS.

Puede monitorizar sus recursos protegidos de una posible actividad de DDoS utilizando Amazon SNS. Para recibir notificaciones de posibles ataques, cree un tema de Amazon para cada región.

Creación de un tema de Amazon SNS en Firewall Manager (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

> **Note**
>
> Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, en FMS de AWS , seleccione Configuración.
3. Elija Create new topic (Crear nuevo tema).
4. Escriba un nombre de tema.
5. Escriba una dirección de correo electrónico a la que se enviarán los mensajes de Amazon SNS y, a continuación, elija Añadir dirección de correo electrónico.
6. Seleccione Update SNS configuration(Actualizar la configuración de SNS).

Configurar las CloudWatch alarmas de Amazon

Shield Advanced registra la detección, la mitigación y las métricas de los principales contribuyentes para CloudWatch que pueda supervisarlas. Para obtener más información, consulteAWS Shield Advanced métricas. CloudWatch incurre en costes adicionales. Para CloudWatch conocer los precios, consulta Amazon CloudWatch Pricing.

Para crear una CloudWatch alarma, sigue las instrucciones de Uso de Amazon CloudWatch Alarms. De forma predeterminada, Shield Advanced se configura CloudWatch para avisarle después de un solo indicador de un posible evento DDoS. Si es necesario, puede usar la CloudWatch consola para cambiar esta configuración y avisarle solo después de que se detecten varios indicadores.

> **Note**
>
> Además de las alarmas, también puede utilizar un CloudWatch panel de control para supervisar la posible actividad de DDoS. El panel recopila y procesa los datos sin formato de Shield Advanced en métricas legibles y casi en tiempo real. Puedes usar las estadísticas de Amazon CloudWatch para obtener una perspectiva del rendimiento de tu aplicación o servicio web. Para obtener más información, consulta Qué hay CloudWatch en la Guía del CloudWatch usuario de Amazon.
>
> Para obtener instrucciones sobre cómo crear un CloudWatch panel de control, consulteMonitorización con Amazon CloudWatch. Para obtener más información acerca de métricas de Shield Advanced específicas que puede añadir a su panel, consulte AWS Shield Advanced métricas.

Cuando haya completado la configuración de Shield Advanced, familiarícese con las opciones de visualización de los eventos en Visibilidad de los eventos de DDoS.

Introducción a las políticas de grupos de seguridad de AWS Firewall Manager Amazon VPC

AWS Firewall Manager Para habilitar los grupos de seguridad de Amazon VPC en toda su organización, lleve a cabo los siguientes pasos en secuencia.

Temas

Paso 1: completar los requisitos previos

Existen varios pasos obligatorios para preparar su cuenta de AWS Firewall Manager. Estos pasos se describen en AWS Firewall Manager requisitos previos. Complete todos los requisitos previos antes de continuar con Paso 2: Crear un grupo de seguridad para utilizarlo en su política.

Paso 2: Crear un grupo de seguridad para utilizarlo en su política

En este paso, creará un grupo de seguridad que podría aplicar en toda la organización mediante Firewall Manager.

> **Note**
>
> En este tutorial, no aplicará la política de grupo de seguridad a los recursos de la organización. Simplemente creará la política y verá qué pasaría si aplicara el grupo de seguridad de la política a sus recursos. Para ello, deshabilitará la corrección automática en la política.

Si ya tiene definido un grupo de seguridad general, omita este paso y vaya a Paso 3: Crear y aplicar una política de grupo de seguridad común.

Creación de un grupo de seguridad para utilizarlo en una política de grupo de seguridad común de Firewall Manager

- Cree un grupo de seguridad que pueda aplicar a todas las cuentas y recursos de la organización, siguiendo las instrucciones que se indican en Grupos de seguridad de su VPC en la Guía de usuario de de Amazon VPC.

  Para obtener información sobre las opciones de reglas de grupo de seguridad, consulte Referencia de reglas de grupos de seguridad.

Ahora está preparado para ir a Paso 3: Crear y aplicar una política de grupo de seguridad común.

Paso 3: Crear y aplicar una política de grupo de seguridad común

Tras completar los requisitos previos, se crea una política de grupo de seguridad AWS Firewall Manager común. Una política de grupo de seguridad común proporciona un grupo de seguridad controlado centralmente para toda AWS la organización. También define los recursos Cuentas de AWS y los recursos a los que se aplica el grupo de seguridad. Además de las políticas de grupos de seguridad comunes, Firewall Manager admite políticas de grupos de seguridad de auditoría de contenido, para administrar las reglas de grupo de seguridad que se utilizan en la organización, y políticas de grupos de seguridad de auditoría de uso, para administrar grupos de seguridad redundantes y no utilizados. Para obtener más información, consulte Políticas de grupos de seguridad.

En este tutorial, creará una política de grupo de seguridad común y la definirá de tal modo que no se corrija automáticamente. Esto le permite ver el efecto que tendría la política sin realizar cambios en su AWS organización.

Creación de una política de grupo de seguridad común de Firewall Manager (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

> **Note**
>
> Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Si no cumple los requisitos previos, la consola muestra instrucciones sobre cómo solucionar cualquier problema. Siga las instrucciones y, a continuación, vuelva a este paso para crear una política de grupo de seguridad común.
4. Elija Crear política.
5. En Policy type (Tipo de política), elija Security group (Grupo de seguridad).
6. En Security group policy type (Tipo de política de grupo de seguridad), elija Common security groups (Grupos de seguridad comunes).
7. En Región, elija una Región de AWS.
8. Elija Siguiente.
9. En Nombre de política, introduzca un nombre descriptivo.
10. Las Policy rules (Reglas de la política) le permiten elegir cómo se aplican y mantienen los grupos de seguridad de esta política. Para este tutorial, deja las opciones sin marcar.
11. Elija Add primary security group (Añadir grupo de seguridad principal), seleccione el grupo de seguridad que ha creado para este tutorial y, a continuación, elija Add security group (Añadir grupo de seguridad).
12. En Policy action (Acción de la política), elija Identify resources that don’t comply with the policy rules, but don’t auto remediate (Identificar los recursos que no cumplan las reglas de la política, pero sin corregirlos automáticamente).
13. Elija Siguiente.
14. Cuentas de AWS afectado por esta política le permite limitar el alcance de su política especificando las cuentas que desea incluir o excluir. En este tutorial, elija Include all accounts under my organization (Incluir todas las cuentas de mi organización).
15. En Tipo de recurso, elija uno o más tipos, según los recursos que haya definido para su AWS organización.
16. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la

inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.

17. Elija Siguiente.
18. En el caso de las etiquetas de política, añada las etiquetas de identificación que desee añadir al recurso de políticas del Firewall Manager. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.
19. Elija Siguiente.
20. Revise la nueva configuración de la política y vuelva a las páginas en las que necesite realizar algún ajuste.

    Compruebe que Acciones de la política está establecido en Identificar los recursos que no cumplan las reglas de la política, pero sin corregirlos automáticamente. Esto te permite revisar los cambios que introduciría tu política antes de activarlos.
21. Cuando esté satisfecho con la política, elija Crear política.

    En el panel de políticas de AWS Firewall Manager , su política debe aparecer en la lista. Probablemente indique Pendiente en los encabezados de cuentas e indique el estado de la configuración de corrección automática. La creación de una política puede tardar varios minutos. Después de reemplazar el estado Pending (Pendiente) por recuentos de cuentas, puede elegir el nombre de la política para explorar el estado de cumplimiento de las cuentas y los recursos. Para obtener información, consulte Visualización de la información de cumplimiento de una AWS Firewall Manager política
22. Cuando haya terminado de explorar, si no desea conservar la política creada para este tutorial, elija el nombre de la política, elija Delete (Eliminar), elija Clean up resources created by this policy (Borrar recursos creados por esta política) y, finalmente, elija Delete (Eliminar).

Para obtener más información acerca de as políticas de grupos de seguridad de Firewall Manager, consulte Políticas de grupos de seguridad.

Introducción a las políticas de ACL de red de AWS Firewall Manager Amazon VPC

AWS Firewall Manager Para habilitar las ACL de red en toda su organización, lleve a cabo los pasos de esta sección de forma secuencial.

Para obtener información sobre las ACL de red, consulte Controlar el tráfico a las subredes mediante las ACL de red en la Guía del usuario de Amazon VPC.

Temas

Paso 1: completar los requisitos previos

Existen varios pasos obligatorios para preparar su cuenta de AWS Firewall Manager. Estos pasos se describen en AWS Firewall Manager requisitos previos. Complete todos los requisitos previos antes de continuar con Paso 2: Crear una política de ACL de red.

Paso 2: Crear una política de ACL de red

Tras cumplir los requisitos previos, debe crear una política de ACL de red de Firewall Manager. Una política de ACL de red proporciona una definición de ACL de red controlada de forma centralizada para toda AWS la organización. También define las subredes Cuentas de AWS y las subredes a las que se aplica la ACL de red.

Para obtener información sobre las políticas de ACL de red de Firewall Manager, consultePolíticas de ACL de red.

Para obtener información general sobre las políticas de ACL de red de Firewall Manager, consultePolíticas de ACL de red.

> **Note**
>
> En este tutorial, no aplicará la política de ACL de red a las subredes de su organización. Solo tendrá que crear la política y ver qué pasaría si aplicara la ACL de red de la política a sus subredes. Para ello, deshabilitará la corrección automática en la política.

Para crear una política ACL de red de Firewall Manager (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Si no cumple los requisitos previos, la consola muestra instrucciones sobre cómo solucionar cualquier problema. Siga las instrucciones y, a continuación, vuelva a este paso para crear una política de ACL de red.
4. Elija Crear política.
5. En Región, elija una Región de AWS.
6. Para el tipo de política, elija Network ACL.
7. Elija Siguiente.
8. En Nombre de política, introduzca un nombre descriptivo.
9. Para las reglas de política de ACL de red, defina la primera y la última regla para el tráfico entrante y saliente.

   Las reglas de ACL de red se definen en Firewall Manager de forma similar a como se definen a través de Amazon VPC. La única diferencia es que, en lugar de asignar los números de regla usted mismo, usted asigna el orden de ejecución de cada conjunto de reglas y, a continuación, Firewall Manager asigna los números por usted al guardar la política. Puede definir hasta 5 reglas de entrada, divididas de cualquier forma entre la primera y la última, y puede definir hasta 5 reglas de salida.

   Para obtener instrucciones sobre cómo especificar las reglas de ACL de red, consulte Añadir y eliminar reglas de ACL de red en la Guía del usuario de Amazon VPC.

   Las reglas que se definen en la política del Firewall Manager especifican la configuración de reglas mínima que debe tener una ACL de red para cumplir con la política de ACL de red. Por ejemplo, las reglas de entrada de una ACL de red no pueden cumplir con la política a menos

que comiencen como las primeras reglas de entrada de la política, en el mismo orden en que se especifican en la política. Para obtener más información, consulte Políticas de ACL de red.

10. En Policy action (Acción de la política), elija Identify resources that don't comply with the policy rules, but don't auto remediate (Identificar los recursos que no cumplan las reglas de la política, pero sin corregirlos automáticamente).
11. Elija Siguiente.
12. Cuentas de AWS La opción afectada por esta política le permite limitar el alcance de la política especificando las cuentas que desee incluir o excluir. En este tutorial, elija Include all accounts under my organization (Incluir todas las cuentas de mi organización).

    El tipo de recurso de una política de ACL de red es siempre subred.
13. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

    Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

    Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.
14. Elija Siguiente.
15. En el caso de las etiquetas de política, añada las etiquetas de identificación que desee añadir al recurso de políticas del Firewall Manager. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.
16. Elija Siguiente.
17. Revise la nueva configuración de la política y vuelva a las páginas en las que necesite realizar algún ajuste.

    Compruebe que Acciones de la política está establecido en Identificar los recursos que no cumplan las reglas de la política, pero sin corregirlos automáticamente. Esto te permite revisar los cambios que introduciría tu política antes de activarlos.
18. Cuando esté satisfecho con la política, elija Crear política.

En el panel de políticas de AWS Firewall Manager , su política debe aparecer en la lista. Probablemente indique Pendiente en los encabezados de cuentas e indique el estado de la configuración de corrección automática. La creación de una política puede tardar varios minutos. Después de reemplazar el estado Pending (Pendiente) por recuentos de cuentas, puede elegir el nombre de la política para explorar el estado de cumplimiento de las cuentas y los recursos. Para obtener información, consulte Visualización de la información de cumplimiento de una AWS Firewall Manager política

19. Cuando haya terminado de explorar, si no desea conservar la política creada para este tutorial, elija el nombre de la política, elija Eliminar, elija Borrar recursos creados por esta política y, finalmente, elija Eliminar.

Para obtener más información sobre las políticas de ACL de red de Firewall Manager, consultePolíticas de ACL de red.

Cómo empezar con AWS Firewall ManagerAWS Network Firewall las políticas

AWS Firewall Manager Para habilitar un firewall de AWS Network Firewall en toda su organización, lleve a cabo los siguientes pasos en secuencia. Para obtener información sobre políticas de Firewall Manager Network Firewall, consulte AWS Network Firewall políticas.

Temas

- Paso 1: Completar los requisitos previos generales
- Paso 2: Crear un grupo de reglas de Network Firewall para usarlo en su política
- Paso 3: Crear y aplicar una política de Network Firewall

Paso 1: Completar los requisitos previos generales

Existen varios pasos obligatorios para preparar su cuenta de AWS Firewall Manager. Estos pasos se describen en AWS Firewall Manager requisitos previos. Complete todos los requisitos previos antes de continuar con el siguiente paso.

Paso 2: Crear un grupo de reglas de Network Firewall para usarlo en su política

Para seguir este tutorial, debe estar familiarizado con sus grupos de reglas AWS Network Firewall y políticas de firewall y saber cómo configurarlos.

Debe tener al menos un grupo de reglas en Network Firewall que se utilizará en su política de AWS Firewall Manager . Si aún no ha creado un grupo de reglas en Network Firewall, hágalo ahora. Para obtener información sobre cómo usar Network Firewall, consulte la Guía para desarrolladores de AWS Network Firewall.

Paso 3: Crear y aplicar una política de Network Firewall

Después de completar los requisitos previos, cree una política de AWS Firewall Manager Network Firewall. Una política de Network Firewall proporciona un AWS Network Firewall firewall controlado centralmente para toda AWS la organización. También define los recursos Cuentas de AWS y los recursos a los que se aplica el firewall.

Para obtener más información sobre cómo Firewall Manager administra sus políticas de Network Firewall, consulte AWS Network Firewall políticas.

Creación de una política de firewall de Firewall Manager Network (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Si no cumple los requisitos previos, la consola muestra instrucciones sobre cómo solucionar cualquier problema. Siga las instrucciones y, a continuación, vuelva a este paso para crear una política de Network Firewall.
4. Seleccione Crear política de seguridad.
5. Para Policy type (Tipo de política), seleccione AWS Network Firewall.
6. En Región, elija una Región de AWS.
7. Elija Siguiente.
8. En Nombre de política, introduzca un nombre descriptivo.

9. La configuración de políticas le permite definir la política de firewall. Es el mismo proceso que se utiliza en la AWS Network Firewall consola. Agregue los grupos de reglas que desea usar en su política y proporcione las acciones sin estado predeterminadas. Para este tutorial, configure esta política como lo haría con una política de firewall en Network Firewall.

   > **Note**
   >
   > La corrección automática se realiza automáticamente para las políticas de AWS Firewall Manager Network Firewall, por lo que aquí no verá ninguna opción para elegir no realizar la corrección automática.

10. Elija Siguiente.
11. Para los puntos de conexión del firewall, seleccione Múltiples puntos de conexión del firewall. Esta opción proporciona una alta disponibilidad para su firewall. Cuando crea la política, Firewall Manager crea una subred de firewall en cada zona de disponibilidad en la que tenga subredes públicas que proteger.
12. En la configuración de rutas de AWS Network Firewall , seleccione Supervisar para que Firewall Manager supervise sus VPC en busca de infracciones de la configuración de rutas y le avise con sugerencias de solución para ayudarle a que las rutas cumplan con las reglas. Opcionalmente, si no desea que Firewall Manager supervise sus configuraciones de rutas y recibir estas alertas, seleccione Desactivado.

    > **Note**
    >
    > La supervisión le proporciona detalles sobre los recursos no compatibles debido a una configuración de ruta defectuosa y sugiere acciones correctivas desde la API `GetViolationDetails` de Firewall Manager. Por ejemplo, Network Firewall le avisa si el tráfico no se enruta a través de los puntos de conexión del firewall creados por su política.

    > **Warning**
    >
    > Si elige Supervisar, no podrá cambiarlo a Desactivado en el futuro para la misma política. Debe crear una política nueva.

13. En el tipo de tráfico, seleccione Agregar a la política de firewall para enrutar el tráfico a través de la puerta de enlace de Internet.
14. Cuentas de AWS La opción afectada por esta política le permite limitar el alcance de la misma especificando las cuentas que desee incluir o excluir. En este tutorial, elija Include all accounts under my organization (Incluir todas las cuentas de mi organización).

    El tipo de recurso para una política de Network Firewall es siempre VPC.
15. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

    Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

    Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.
16. Elija Siguiente.
17. En el caso de las etiquetas de política, añada las etiquetas de identificación que desee añadir al recurso de políticas del Firewall Manager. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.
18. Elija Siguiente.
19. Revise la nueva configuración de la política y vuelva a las páginas en las que necesite realizar algún ajuste.

    Compruebe que Acciones de la política está establecido en Identificar los recursos que no cumplan las reglas de la política, pero sin corregirlos automáticamente. Esto te permite revisar los cambios que introduciría tu política antes de activarlos.
20. Cuando esté satisfecho con la política, elija Crear política.

    En el panel de políticas de AWS Firewall Manager , su política debe aparecer en la lista. Probablemente indique Pendiente en los encabezados de cuentas e indique el estado de la configuración de corrección automática. La creación de una política puede tardar varios minutos. Después de reemplazar el estado Pending (Pendiente) por recuentos de cuentas, puede elegir el nombre de la política para explorar el estado de cumplimiento de las cuentas y los recursos.

Para obtener información, consulte Visualización de la información de cumplimiento de una AWS Firewall Manager política

21. Cuando haya terminado de explorar, si no desea conservar la política creada para este tutorial, elija el nombre de la política, elija Eliminar, elija Borrar recursos creados por esta política y, finalmente, elija Eliminar.

Para más información sobre políticas de Firewall Manager Network Firewall, consulte AWS Network Firewall políticas.

Introducción a las políticas de firewall de AWS Firewall Manager DNS

AWS Firewall Manager Para habilitar el firewall DNS Amazon Route 53 Resolver en toda su organización, lleve a cabo los siguientes pasos en secuencia. Para obtener información acerca de las políticas de Firewall Manager DNS Firewall, consulte Políticas de DNS firewall de Amazon Route 53 Resolver.

Temas

- Paso 1: Completar los requisitos previos generales
- Paso 2: Crear su grupo de reglas de DNS Firewall para usarlo en su política
- Paso 3: Crear y aplicar una política de DNS Firewall

Paso 1: Completar los requisitos previos generales

Existen varios pasos obligatorios para preparar su cuenta de AWS Firewall Manager. Estos pasos se describen en AWS Firewall Manager requisitos previos. Complete todos los requisitos previos antes de continuar con el siguiente paso.

Paso 2: Crear su grupo de reglas de DNS Firewall para usarlo en su política

Para seguir este tutorial, debe estar familiarizado con Amazon Route 53 Resolver DNS Firewall y saber cómo configurar sus grupos de reglas.

Debe tener al menos un grupo de reglas en DNS Firewall que se utilizará en su política de AWS Firewall Manager . Si aún no ha creado un grupo de reglas en DNS Firewall, hágalo ahora. Para obtener información sobre el uso de DNS Firewall, consulte Amazon Route 53 Resolver DNS Firewall en la Guía para desarrolladores de Amazon Route 53.

Paso 3: Crear y aplicar una política de DNS Firewall

Tras completar los requisitos previos, se crea una política de firewall de AWS Firewall Manager DNS. Una política de firewall de DNS proporciona un conjunto de asociaciones de grupos de reglas de firewall de DNS controladas de forma centralizada para toda AWS la organización. También define las Cuentas de AWS y recursos a los que se aplica el firewall.

Para obtener más información sobre cómo administra Firewall Manager sus asociaciones de grupos de reglas de DNS Firewall, consulte Políticas de DNS firewall de Amazon Route 53 Resolver.

Creación de una política de DNS Firewall de Firewall Manager (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.
2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Si no cumple los requisitos previos, la consola muestra instrucciones sobre cómo solucionar cualquier problema. Siga las instrucciones y, a continuación, vuelva a este paso para crear una política de DNS Firewall.
4. Seleccione Crear política de seguridad.
5. En Tipo de política, elija Amazon Route 53 Resolver DNS Firewall.
6. En Región, elija una Región de AWS.
7. Elija Siguiente.
8. En Nombre de política, introduzca un nombre descriptivo.
9. La configuración de la política le permite definir las asociaciones de grupos de reglas de DNS Firewall que desea administrar desde Firewall Manager. Agregue los grupos de reglas que desee utilizar en su política. Puede definir qué asociación de sus VPC se evalúa primero y cuál en último lugar. Para este tutorial, añada una o dos asociaciones de grupos de reglas, según sus necesidades.
10. Elija Siguiente.
11. Cuentas de AWS afectado por esta política le permite limitar el alcance de su política especificando las cuentas que desea incluir o excluir. En este tutorial, elija Include all accounts under my organization (Incluir todas las cuentas de mi organización).

    El tipo de recurso para una política de DNS Firewall es siempre VPC.

12. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

    Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

    Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.

13. Elija Siguiente.

14. En el caso de las etiquetas de política, añada las etiquetas de identificación que desee añadir al recurso de políticas del Firewall Manager. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

15. Elija Siguiente.

16. Revise la nueva configuración de la política y vuelva a las páginas en las que necesite realizar algún ajuste.

    Compruebe que Acciones de la política está establecido en Identificar los recursos que no cumplan las reglas de la política, pero sin corregirlos automáticamente. Esto te permite revisar los cambios que introduciría tu política antes de activarlos.

17. Cuando esté satisfecho con la política, elija Crear política.

    En el panel de políticas de AWS Firewall Manager , su política debe aparecer en la lista. Probablemente indique Pendiente en los encabezados de cuentas e indique el estado de la configuración de corrección automática. La creación de una política puede tardar varios minutos. Después de reemplazar el estado Pending (Pendiente) por recuentos de cuentas, puede elegir el nombre de la política para explorar el estado de cumplimiento de las cuentas y los recursos. Para obtener información, consulte Visualización de la información de cumplimiento de una AWS Firewall Manager política

18. Cuando haya terminado de explorar, si no desea conservar la política creada para este tutorial, elija el nombre de la política, elija Eliminar, elija Borrar recursos creados por esta política y, finalmente, elija Eliminar.

Para obtener más información acerca de las políticas de Firewall Manager DNS Firewall, consulte Políticas de DNS firewall de Amazon Route 53 Resolver.

Cómo empezar con las políticas de firewall de próxima generación de AWS Firewall Manager Palo Alto Networks Cloud

AWS Firewall Manager Para habilitar las políticas de firewall de próxima generación (NGFW) de Palo Alto Networks Cloud, lleve a cabo los siguientes pasos en secuencia. Para obtener información sobre las políticas de NGFW en la nube de Palo Alto Networks, consulte Políticas de NGFW en la nube de Palo Alto Networks.

Temas

- Paso 1: Completar los requisitos previos generales
- Paso 2: Completar los requisitos previos de la política de NGFW en la nube de Palo Alto Networks
- Paso 3: Crear y aplicar una política de NGFW en la nube de Palo Alto Networks

Paso 1: Completar los requisitos previos generales

Existen varios pasos obligatorios para preparar su cuenta de AWS Firewall Manager. Estos pasos se describen en AWS Firewall Manager requisitos previos. Complete todos los requisitos previos antes de continuar con el siguiente paso.

Paso 2: Completar los requisitos previos de la política de NGFW en la nube de Palo Alto Networks

Para poder utilizar las políticas de NGFW en la nube de Palo Alto Networks, debe completar un par de pasos obligatorios adicionales. Estos pasos se describen en Requisitos previos de la política de firewall de próxima generación de Palo Alto Networks Cloud. Complete todos los requisitos previos antes de continuar con el siguiente paso.

Paso 3: Crear y aplicar una política de NGFW en la nube de Palo Alto Networks

Tras completar los requisitos previos, debe crear una política de NGFW en la nube de AWS Firewall Manager Palo Alto Networks.

Para obtener más información sobre las políticas de Firewall Manager para NGFW en la nube de Palo Alto Networks, consulte Políticas de NGFW en la nube de Palo Alto Networks.

Creación de una política de Firewall Manager para NGFW en la nube de Palo Alto Networks (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Elija Crear política.
4. Para el tipo de política, elija Palo Alto Networks Cloud NGFW. Si aún no te has suscrito al servicio NGFW en la nube de Palo Alto Networks en AWS Marketplace, tendrás que hacerlo primero. Para suscribirte en AWS Marketplace, selecciona Ver detalles del AWS Marketplace.
5. Para Modelo de implementación, elija Modelo distribuido o Modelo centralizado. El modelo de implementación determina la forma en que Firewall Manager administra los puntos de conexión de la política. Con el modelo distribuido, Firewall Manager mantiene los puntos de conexión del firewall en cada VPC que se encuentre dentro del ámbito de aplicación de la política. Con el modelo centralizado, Firewall Manager mantiene un único punto de conexión en una VPC de inspección.
6. En Región, selecciona una Región de AWS. Para proteger los recursos en varias regiones, debe crear políticas distintas para cada región.
7. Elija Siguiente.
8. En Nombre de política, introduzca un nombre descriptivo.
9. En la configuración de la política, elija la política de firewall de NGFW en la nube de Palo Alto Networks para asociarla a esta política. La lista de políticas de firewall de NGFW en la nube de Palo Alto Networks contiene todas las políticas de firewall de NGFW en la nube de Palo Alto Networks asociadas a su inquilino de NGFW en la nube de Palo Alto Networks. Para obtener información sobre cómo crear y administrar las políticas de firewall de NGFW en la nube de Palo Alto Networks, consulte la guía Implemente el NGFW en la nube de Palo Alto Networks, que incluye el AWS Firewall Manager tema en la AWS guía de implementación del NGFW en la nube de Palo Alto Networks. AWS

10. Para el registro de NGFW en Palo Alto Networks Cloud (opcional), elija los tipos de registro de NGFW de Palo Alto Networks Cloud que desee registrar para su política. Para obtener información sobre los tipos de registro del NGFW en la nube de Palo Alto Networks, consulte Configurar el registro del NGFW en la nube de Palo Alto Networks en la guía de implementación del NGFW AWS en la nube de Palo Alto Networks. AWS

    En Destino del registro, especifique en qué momento Firewall Manager debe escribir los registros.

11. Elija Siguiente.
12. En Configurar punto de conexión de firewall de terceros, lleve a cabo una de las siguientes acciones, en función de si utiliza el modelo de implementación distribuido o centralizado para crear los puntos de conexión de firewall:

    - Si utiliza el modelo de implementación distribuida para esta política, en Zonas de disponibilidad, seleccione en qué zonas de disponibilidad desea crear los puntos de conexión del firewall. Puede seleccionar las zonas de disponibilidad por Nombre de la zona de disponibilidad o por ID de la zona de disponibilidad.
    - Si utiliza el modelo de implementación centralizada para esta política, en Configuración de punto de conexión de AWS Firewall Manager de Configuración de VPC de inspección, introduzca el ID de cuenta de AWS del propietario de la VPC de inspección y el ID de VPC de la VPC de inspección.
        - En Zonas de disponibilidad, seleccione en qué zonas de disponibilidad desea crear los puntos de conexión del firewall. Puede seleccionar las zonas de disponibilidad por Nombre de la zona de disponibilidad o por ID de la zona de disponibilidad.

13. Elija Siguiente.
14. Para Alcance de la política, en esta política se aplica a Cuentas de AWS , elija la opción siguiente:

    - Si desea aplicar la política a todas las cuentas de su organización, deje la selección predeterminada, Incluir todas las cuentas de mi organización. AWS
    - Si desea aplicar la política solo a cuentas específicas o a cuentas que se encuentran en unidades AWS Organizations organizativas (OU) específicas, elija Incluir solo las cuentas y unidades organizativas especificadas y, a continuación, agregue las cuentas y las OU que desee incluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.

- Si desea aplicar la política a todas las cuentas o unidades AWS Organizations organizativas (OU) excepto a un conjunto específico, elija Excluir las cuentas y unidades organizativas especificadas e incluir todas las demás y, a continuación, agregue las cuentas y unidades organizativas que desee excluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.

Solo puede elegir una de las opciones.

Después de aplicar la política, Firewall Manager evalúa automáticamente las cuentas nuevas en función de la configuración. Por ejemplo, si solo incluye cuentas específicas, Firewall Manager no aplica la política a ninguna cuenta nueva. Como otro ejemplo, si incluye una unidad organizativa, cuando agrega una cuenta a la unidad organizativa o a cualquiera de sus unidades organizativas secundarias, Firewall Manager aplica automáticamente la política a la nueva cuenta.

El Tipo de recurso para las políticas de Network Firewall es VPC.

15. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

    Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

    Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.

16. En Conceder acceso entre cuentas, seleccione Descargar plantilla de AWS CloudFormation . Esto descarga una AWS CloudFormation plantilla que puedes usar para crear una AWS CloudFormation pila. Esta pila crea un AWS Identity and Access Management rol que otorga permisos entre cuentas a Firewall Manager para administrar los recursos de NGFW en la nube de Palo Alto Networks. Para obtener información acerca de las pilas, consulte Uso de pilas en la Guía del usuario de AWS CloudFormation .
17. Elija Siguiente.

18. En el caso de las etiquetas de política, añada las etiquetas de identificación que desee añadir al recurso de políticas del Firewall Manager. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.
19. Elija Siguiente.
20. Revise la nueva configuración de la política y vuelva a las páginas en las que necesite realizar algún ajuste.

    Compruebe que Acciones de la política está establecido en Identificar los recursos que no cumplan las reglas de la política, pero sin corregirlos automáticamente. Esto te permite revisar los cambios que introduciría tu política antes de activarlos.
21. Cuando esté satisfecho con la política, elija Crear política.

    En el panel de políticas de AWS Firewall Manager , su política debe aparecer en la lista. Probablemente indique Pendiente en los encabezados de cuentas e indique el estado de la configuración de corrección automática. La creación de una política puede tardar varios minutos. Después de reemplazar el estado Pending (Pendiente) por recuentos de cuentas, puede elegir el nombre de la política para explorar el estado de cumplimiento de las cuentas y los recursos. Para obtener información, consulte Visualización de la información de cumplimiento de una AWS Firewall Manager política

Para obtener más información sobre las políticas de NGFW en la nube de Firewall Manager de Palo Alto Networks, consulte Políticas de NGFW en la nube de Palo Alto Networks.

Cómo empezar con las políticas de AWS Firewall Manager Fortigate CNF

El firewall nativo en la nube (CNF) de Fortigate como servicio es un servicio de firewall de terceros que puede utilizar para sus políticas. AWS Firewall Manager Con Fortigate CNF para Firewall Manager, puede crear e implementar de forma centralizada los recursos y conjuntos de políticas de Fortigate CNF en todas sus cuentas. AWS AWS Firewall Manager Para habilitar las políticas de CNF de Fortigate, lleve a cabo los siguientes pasos en secuencia. Para obtener más información sobre las políticas Fortigate CNF, consulte Políticas de Fortigate Cloud Native Firewall (CNF) como servicio.

Temas

- Paso 1: Completar los requisitos previos generales
- Paso 2: Completar los requisitos previos de políticas de Fortigate CNF
- Paso 3: Crear y aplicar una política de Fortigate CNF

Paso 1: Completar los requisitos previos generales

Existen varios pasos obligatorios para preparar su cuenta de AWS Firewall Manager. Estos pasos se describen en AWS Firewall Manager requisitos previos. Complete todos los requisitos previos antes de continuar con el siguiente paso.

Paso 2: Completar los requisitos previos de políticas de Fortigate CNF

Hay otros pasos obligatorios que debe completar para poder utilizar las políticas de Fortigate CNF. Estos pasos se describen en Requisitos previos de la política de firewall nativo en la nube (CNF) de Fortigate como servicio. Complete todos los requisitos previos antes de continuar con el siguiente paso.

Paso 3: Crear y aplicar una política de Fortigate CNF

Tras completar los requisitos previos, debe crear una política de CNF de AWS Firewall Manager Fortigate.

Para obtener más información sobre las políticas de Firewall Manager para Fortigate CNF, consulte Políticas de Fortigate Cloud Native Firewall (CNF) como servicio.

Creación de una política de Firewall Manager para Fortigate CNF (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Elija Crear política.
4. Para Tipo de política, seleccione Fortigate CNF. Si aún no se ha suscrito al servicio Fortigate CNF en el AWS Marketplace, primero tendrá que hacerlo. Para suscribirte en AWS Marketplace, selecciona Ver detalles del AWS Marketplace.

5. Para Modelo de implementación, elija Modelo distribuido o Modelo centralizado. El modelo de implementación determina la forma en que Firewall Manager administra los puntos de conexión de la política. Con el modelo distribuido, Firewall Manager mantiene los puntos de conexión del firewall en cada VPC que se encuentre dentro del ámbito de aplicación de la política. Con el modelo centralizado, Firewall Manager mantiene un único punto de conexión en una VPC de inspección.
6. En Región, selecciona una Región de AWS. Para proteger los recursos en varias regiones, debe crear políticas distintas para cada región.
7. Elija Siguiente.
8.
9. En la configuración de la política, elija la política de firewall Fortigate CNF para asociarla a esta política. La lista de políticas de firewall de Fortigate CNF contiene todas las políticas de firewall de Fortigate CNF asociadas a su inquilino de Fortigate CNF. Para obtener información sobre cómo crear y administrar las políticas de firewall de Fortigate CNF, consulte la documentación de Fortigate CNF.
10. Elija Siguiente.
11. En Configurar punto de conexión de firewall de terceros, lleve a cabo una de las siguientes acciones, en función de si utiliza el modelo de implementación distribuido o centralizado para crear los puntos de conexión de firewall:

    - Si utiliza el modelo de implementación distribuida para esta política, en Zonas de disponibilidad, seleccione en qué zonas de disponibilidad desea crear los puntos de conexión del firewall. Puede seleccionar las zonas de disponibilidad por Nombre de la zona de disponibilidad o por ID de la zona de disponibilidad.
    - Si utiliza el modelo de implementación centralizada para esta política, en Configuración de punto de conexión de AWS Firewall Manager de Configuración de VPC de inspección, introduzca el ID de cuenta de AWS del propietario de la VPC de inspección y el ID de VPC de la VPC de inspección.
        - En Zonas de disponibilidad, seleccione en qué zonas de disponibilidad desea crear los puntos de conexión del firewall. Puede seleccionar las zonas de disponibilidad por Nombre de la zona de disponibilidad o por ID de la zona de disponibilidad.
12. Elija Siguiente.
13. Para Alcance de la política, en esta política se aplica a Cuentas de AWS , elija la opción siguiente:

- Si desea aplicar la política a todas las cuentas de su organización, deje la selección predeterminada, Incluir todas las cuentas de mi AWS organización.
- Si desea aplicar la política solo a cuentas específicas o a cuentas que se encuentran en unidades AWS Organizations organizativas (OU) específicas, elija Incluir solo las cuentas y unidades organizativas especificadas y, a continuación, agregue las cuentas y las OU que desee incluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.
- Si desea aplicar la política a todas las cuentas o unidades AWS Organizations organizativas (OU) excepto a un conjunto específico, elija Excluir las cuentas y unidades organizativas especificadas e incluir todas las demás y, a continuación, agregue las cuentas y unidades organizativas que desee excluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.

Solo puede elegir una de las opciones.

Después de aplicar la política, Firewall Manager evalúa automáticamente las cuentas nuevas en función de la configuración. Por ejemplo, si solo incluye cuentas específicas, Firewall Manager no aplica la política a ninguna cuenta nueva. Como otro ejemplo, si incluye una unidad organizativa, cuando agrega una cuenta a la unidad organizativa o a cualquiera de sus unidades organizativas secundarias, Firewall Manager aplica automáticamente la política a la nueva cuenta.

El tipo de recurso para las políticas CNF de Fortigate es VPC.

14. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

    Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.

15. En Conceder acceso entre cuentas, seleccione Descargar plantilla de AWS CloudFormation . Esto descarga una AWS CloudFormation plantilla que puedes usar para crear una AWS CloudFormation pila. Esta pila crea un AWS Identity and Access Management rol que otorga permisos multicuenta al Administrador de Firewall para administrar los recursos de Fortigate CNF. Para obtener información acerca de las pilas, consulte Uso de pilas en la Guía del usuario de AWS CloudFormation . Para crear una pila, necesitará el ID de cuenta del portal de Fortigate CNF.
16. Elija Siguiente.
17. En el caso de las etiquetas de política, añada las etiquetas de identificación que desee añadir al recurso de políticas del Firewall Manager. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.
18. Elija Siguiente.
19. Revise la nueva configuración de la política y vuelva a las páginas en las que necesite realizar algún ajuste.

    Compruebe que Acciones de la política está establecido en Identificar los recursos que no cumplan las reglas de la política, pero sin corregirlos automáticamente. Esto te permite revisar los cambios que introduciría tu política antes de activarlos.
20. Cuando esté satisfecho con la política, elija Crear política.

    En el panel de políticas de AWS Firewall Manager , su política debe aparecer en la lista. Probablemente indique Pendiente en los encabezados de cuentas e indique el estado de la configuración de corrección automática. La creación de una política puede tardar varios minutos. Después de reemplazar el estado Pending (Pendiente) por recuentos de cuentas, puede elegir el nombre de la política para explorar el estado de cumplimiento de las cuentas y los recursos. Para obtener información, consulte Visualización de la información de cumplimiento de una AWS Firewall Manager política

Para obtener más información sobre las políticas Fortigate CNF de Firewall Manager, consulte Políticas de Fortigate Cloud Native Firewall (CNF) como servicio.

Trabajar con AWS Firewall Manager políticas

AWS Firewall Manager proporciona los siguientes tipos de políticas. Para cada tipo de política, debe definir lo siguiente:

- AWS WAFpolítica: Firewall Manager admite AWS WAF políticas AWS WAF clásicas. Para ambas versiones, defina qué recursos están protegidos por la política.
  - El tipo AWS WAF de política requiere que los conjuntos de grupos de reglas se ejecuten primero y último en la ACL web. Luego, en las cuentas en las que se aplica la ACL web, el propietario de la cuenta puede agregar reglas y grupos de reglas para que se ejecuten entre los dos conjuntos.
  - El tipo de política AWS WAF clásica requiere un único grupo de reglas para ejecutarse en la ACL web.
- Política Shield Advanced: este tipo de política aplica las protecciones Shield Advanced en toda la organización para los tipos de recursos que especifique.
- Política de grupos de seguridad de Amazon VPC: este tipo de política le permite controlar los grupos de seguridad que se utilizan en toda la organización y le permite aplicar un conjunto básico de reglas en toda la organización.
- Política de listas de control de acceso a la red (ACL) de Amazon VPC: este tipo de política le permite controlar las ACL de red que se utilizan en toda la organización y le permite aplicar un conjunto básico de ACL de red en toda la organización.
- Política de Network Firewall: este tipo de política aplica AWS Network Firewall protección a las VPC de su organización.
- Política de firewall de DNS de Amazon Route 53 Resolver: esta política aplica las protecciones de DNS Firewall a las VPC de su organización.
- Política de firewall de terceros: este tipo de política aplica protecciones de firewall de terceros. Los firewalls de terceros están disponibles mediante suscripción a través de la consola AWS Marketplace en AWS Marketplace.
  - Política de NGFW de Palo Alto Networks Cloud: este tipo de política aplica las protecciones del firewall de próxima generación (NGFW) de Palo Alto Networks Cloud y las normas de NGFW de Palo Alto Networks Cloud a las VPC de su organización.
  - Política de firewall nativo de Fortigate Cloud (CNF) como servicio: este tipo de política aplica las protecciones del firewall nativo de Fortigate Cloud (CNF) como servicio. Fortigate CNF es una solución centrada en la nube que bloquea las amenazas de día cero y protege las infraestructuras en la nube con una prevención de amenazas avanzada líder del sector, firewalls de aplicaciones web inteligentes (WAF) y protección mediante API.

Una política de Firewall Manager es específica del tipo de política individual. Si desea aplicar varios tipos de políticas en diversas cuentas, puede crear varias políticas. Puede crear más de una política para cada tipo.

Si agrega una cuenta nueva a una organización con la que creó AWS Organizations, Firewall Manager aplicará automáticamente la política a los recursos de esa cuenta que estén dentro del ámbito de la política.

Configuración general de las AWS Firewall Manager políticas

AWS Firewall Manager las políticas gestionadas tienen algunos ajustes y comportamientos comunes. En todas ellas se especifica un nombre y se define el alcance de la política, y se puede utilizar el etiquetado de recursos para controlar el alcance de la política. Puede elegir ver las cuentas y los recursos que están en situación de incumplimiento sin tomar medidas correctivas o corregir automáticamente los recursos en situación de incumplimiento.

Para obtener información sobre el alcance de la política, consulte AWS Firewall Manager alcance de la política.

Creación de una AWS Firewall Manager política

Los pasos para crear una política varían entre los diferentes tipos de políticas. Asegúrese de utilizar el procedimiento adecuado para el tipo de política que necesita.

> **Important**
>
> AWS Firewall Manager no es compatible con Amazon Route 53 o AWS Global Accelerator. Si desea proteger estos recursos con Shield Advanced, no puede utilizar una política de Firewall Manager. En su lugar, siga las instrucciones en Añadir AWS Shield Advanced protección a AWS los recursos.

Temas

- Crear una AWS Firewall Manager política para AWS WAF
- Crear una AWS Firewall Manager política para Classic AWS WAF
- Crear una AWS Firewall Manager política para AWS Shield Advanced
- Crear una política de grupo de seguridad común de AWS Firewall Manager
- Crear una política de grupo de seguridad de auditoría de contenido de AWS Firewall Manager

- Crear una política de grupo de seguridad de auditoría de uso de AWS Firewall Manager
- Crear una política AWS Firewall Manager de ACL de red
- Crear una AWS Firewall Manager política para AWS Network Firewall
- Creación de una AWS Firewall Manager política para Amazon Route 53 Resolver DNS Firewall
- Creación de una AWS Firewall Manager política para el NGFW en la nube de Palo Alto Networks
- Crear una AWS Firewall Manager política para Fortigate Cloud Native Firewall (CNF) como servicio

Crear una AWS Firewall Manager política para AWS WAF

En una AWS WAF política de Firewall Manager, puedes usar grupos de reglas gestionados, que AWS AWS Marketplace los vendedores crean y mantienen por ti. También puede crear y utilizar sus propios grupos de reglas. Para obtener más información acerca de los grupos de reglas, consulte AWS WAF grupos de reglas.

Si desea utilizar sus propios grupos de reglas, créelos antes de crear su política de Firewall Manager de AWS WAF . Para obtener instrucciones, consulte Administrar sus propios grupos de reglas. Para utilizar una regla personalizada individual, debe definir su propio grupo de reglas, definir la regla dentro de él y, a continuación, utilizar el grupo de reglas en la política.

Para obtener información sobre AWS WAF las políticas de Firewall Manager, consulteAWS WAF políticas.

Para crear una política de Firewall Manager para AWS WAF (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Elija Crear política.
4. Para Policy type (Tipo de política), seleccione AWS WAF.

5. En Región, elija una Región de AWS. Para proteger CloudFront las distribuciones de Amazon, elige Global.

   Para proteger los recursos en varias regiones (distintas de CloudFront las distribuciones), debe crear políticas de Firewall Manager independientes para cada región.

6. Elija Siguiente.

7. En Nombre de política, introduzca un nombre descriptivo. Firewall Manager incluye el nombre de la política en los nombres de las ACL web que administra. Los nombres de las ACL web `FMManagedWebACLV2-` van seguidos del nombre de la política que se introduce aquí, `-`, y de la marca temporal de creación de las ACL web, en milisegundos UTC. Por ejemplo, `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`.

8. Para inspeccionar el cuerpo de las solicitudes web, si lo desea, puede cambiar el límite de tamaño corporal. Para obtener información sobre los límites de tamaño para la inspección corporal, incluidas las consideraciones de precio, consulte Gestión de los límites de tamaño de la inspección corporal en la Guía para desarrolladores de AWS WAF .

9. En Reglas de políticas, agregue los grupos de reglas que desee AWS WAF evaluar primero y último en la ACL web. Para usar el control de versiones de grupos de reglas AWS WAF administrado, active la opción Habilitar el control de versiones. Los administradores de cuentas individuales pueden agregar reglas y grupos de reglas entre los primeros grupos de reglas y los últimos grupos de reglas. Para obtener más información sobre el uso de grupos de AWS WAF reglas en las políticas del Firewall Manager AWS WAF, consulteAWS WAF políticas.

   (Opcional) Para personalizar la forma en que su ACL web utiliza el grupo de reglas, seleccione Editar. A continuación se muestra la configuración de personalización común:

   - En el caso de los grupos de reglas administradas, anule las acciones de las reglas para algunas o todas las reglas. Si no define una acción de anulación para una regla, la evaluación utiliza la acción de la regla que está definida dentro del grupo de reglas. Para obtener información acerca de esta opción, consulte Opciones de anulación de acciones para grupos de reglas en la Guía para desarrolladores de AWS WAF .
   - Algunos grupos de reglas administradas requieren que se proporcione una configuración adicional. Consulte la documentación de su proveedor de grupos de reglas administradas. Para obtener información específica sobre los grupos de reglas de reglas AWS administradas, consulte AWS Reglas administradas para AWS WAF la Guía para AWS WAF desarrolladores.

   Cuando haya terminado con la configuración, seleccione Guardar regla.

10. Establezca la acción predeterminada para la ACL web. Esta es la acción que realiza el AWS WAF cuando una solicitud web no coincide con ninguna de las reglas de la ACL web. Puede añadir encabezados personalizados con la acción Permitir o respuestas personalizadas para la acción Bloquear. Para obtener más información acerca de las acciones ACL web predeterminadas, consulte La acción predeterminada de ACL web. Para obtener información sobre cómo configurar las solicitudes y respuestas web personalizadas, consulte Solicitudes web y respuestas personalizadas en AWS WAF.
11. Para la configuración del registro, seleccione Habilitar el registro para activar el registro. El registro ofrece obtener información detallada sobre el tráfico que analiza su ACL web. Seleccione el destino del registro y, a continuación, seleccione el destino del registro que haya configurado. Debe elegir un destino de registro cuyo nombre comience con `aws-waf-logs-`. Para obtener información sobre la configuración de un destino de AWS WAF registro, consulteConfigurar el registro para una AWS WAF política.
12. (Opcional) Si no desea determinados campos y sus valores incluidos en los registros, redacte esos campos. Elija el campo que se va a redactar y, a continuación, elija Add (Añadir). Repita según sea necesario para redactar campos adicionales. Los campos redactados aparecen como `REDACTED` en los registros. Por ejemplo, si redacta el campo URI, el campo URI de los registros será `REDACTED`.
13. (Opcional) Si no desea enviar todas las solicitudes a los registros, agregue sus criterios de filtrado y su comportamiento. En Filtrar registros, para cada filtro que desee aplicar, elija Agregar filtro y, a continuación, elija sus criterios de filtrado y especifique si desea conservar o eliminar las solicitudes que coincidan con los criterios. Cuando termine de agregar los filtros, si es necesario, modifique el comportamiento de registro predeterminado. Para obtener más información, consulte Configuración de registro de ACL web en la Guía para desarrolladores de AWS WAF .
14. Puede definir una lista de dominios de token para permitir el intercambio de tokens entre aplicaciones protegidas. Las Challenge acciones CAPTCHA y los SDK de integración de aplicaciones que se implementan cuando se utilizan los grupos de reglas de AWS Managed Rules para el control del AWS WAF fraude, la prevención de apropiación de cuentas (ATP) y el control de AWS WAF bots utilizan los tokens.

    No se admiten sufijos públicos. Por ejemplo, no puede usar `gov.au` o `co.uk` como dominio de token.

    De forma predeterminada, solo AWS WAF acepta los tokens del dominio del recurso protegido. Si agrega dominios simbólicos a esta lista, AWS WAF acepta los tokens para todos los dominios

de la lista y para el dominio del recurso asociado. Para obtener más información, consulte AWS WAF Configuración de la lista de dominios del token ACL web en la Guía para desarrolladores de AWS WAF .

Solo puede cambiar el CAPTCHA de la ACL web y desafiar los tiempos de inmunidad al editar una ACL web existente. Puede encontrar esta configuración en la página de Detalles de las políticas del Firewall Manager. Para obtener más información sobre esta configuración, consulte Caducidad de la marca de tiempo: tiempos de inmunidad AWS WAF simbólica. Si actualiza la configuración de la asociación, el CAPTCHA, el desafío o la lista de dominios de token en una política existente, Firewall Manager sobrescribirá las ACL web locales con los nuevos valores. Sin embargo, si no actualiza la configuración de asociación, el CAPTCHA, el desafío o la lista de dominios de token de la política, los valores de las ACL web locales permanecerán inalterados. Para obtener información acerca de esta opción, consulte CAPTCHAy Challenge en AWS WAF en la Guía para desarrolladores de AWS WAF .

15. En Administración de ACL web, si desea que Firewall Manager administre las ACL web no asociadas, habilite Administrar ACL web no asociadas. Con esta opción, Firewall Manager crea ACL web en las cuentas dentro del alcance de la política solo si las ACL web serán utilizadas por al menos un recurso. Si en algún momento, una cuenta entra en el alcance de la política, Firewall Manager crea automáticamente una ACL web en la cuenta si al menos un recurso utilizará la ACL web. Al activar esta opción, el Firewall Manager realiza una limpieza única de las ACL web no asociadas de su cuenta. El proceso de limpieza puede tardar varias horas. Si un recurso sale del alcance de la política después de que el Firewall Manager haya creado una ACL web, el Firewall Manager disociará el recurso de la ACL web, pero no realizará la limpieza de la ACL web no asociada. Firewall Manager solo realiza la limpieza de las ACL web no asociadas cuando se habilita por primera vez la administración de las ACL web no asociadas en una política.
16. Para Acción de política, si desea crear una ACL web en cada cuenta aplicable dentro de la organización, pero no aplicar la ACL web a ningún recurso todavía, elija Identificar recursos que no cumplan las reglas de la política, pero que no se corrijan automáticamente y no elija Administrar ACL web no asociadas. Puede cambiar estas opciones más adelante.

    Si, en su lugar, desea aplicar automáticamente la política a los recursos existentes dentro del ámbito, elija Auto remediate any noncompliant resources (Solucionar automáticamente los recursos no conformes). Si la opción Administrar ACL web no asociadas está desactivada, la opción Corregir automáticamente los recursos no compatibles crea una ACL web en cada cuenta aplicable de la organización y asocia la ACL web a los recursos de las cuentas. Si la opción Administrar ACL web no asociadas está habilitada, la opción Corregir automáticamente

los recursos no compatibles solo crea y asocia una ACL web en las cuentas que tienen recursos aptos para asociarse a la ACL web.

Al elegir Corregir automáticamente los recursos no compatibles, también puede optar por eliminar las asociaciones existentes de ACL web de los recursos pertinentes, para aquellas ACL web que no estén administradas por otra política activa de Firewall Manager. Si elige este opción, Firewall Manager asociará primero la ACL web de la política con los recursos y después quitará las asociaciones anteriores. Si un recurso tiene una asociación con otra ACL web administrada por una política de Firewall Manager activa diferente, esta opción no afectará a esa asociación.

17. Elija Siguiente.
18. En Cuentas de AWS a las que se aplica esta política, elija la opción de la siguiente manera:

    - Si desea aplicar la política a todas las cuentas de su organización, deje la selección predeterminada, Incluir todas las cuentas de mi AWS organización.
    - Si desea aplicar la política solo a cuentas específicas o a cuentas que se encuentran en unidades AWS Organizations organizativas (OU) específicas, elija Incluir solo las cuentas y unidades organizativas especificadas y, a continuación, agregue las cuentas y OU que desee incluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.
    - Si desea aplicar la política a todas las cuentas o unidades organizativas (OU) de AWS Organizations excepto a un conjunto específico, elija Exclude the specified accounts and organizational units, and include all others (Excluir las cuentas y unidades organizativas especificadas e incluir todas las demás), y, a continuación, agregue las cuentas y unidades organizativas que desee excluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.

    Solo puede elegir una de las opciones.

    Después de aplicar la política, Firewall Manager evalúa automáticamente las cuentas nuevas en función de la configuración. Por ejemplo, si solo incluye cuentas específicas, Firewall Manager no aplica la política a ninguna cuenta nueva. Como otro ejemplo, si incluye una unidad organizativa, cuando agrega una cuenta a la unidad organizativa o a cualquiera de sus unidades

organizativas secundarias, Firewall Manager aplica automáticamente la política a la nueva cuenta.

19. En Resource type (Tipo de recurso), elija los tipos de recurso que desea proteger.
20. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

    Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

    Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.
21. Elija Siguiente.
22. En el caso de las etiquetas de política, añada las etiquetas de identificación que desee añadir al recurso de políticas del Firewall Manager. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.
23. Elija Siguiente.
24. Revise la nueva configuración de la política y vuelva a las páginas en las que necesite realizar algún ajuste.

    Cuando esté satisfecho con la política, elija Crear política. En el panel de políticas de AWS Firewall Manager , su política debe aparecer en la lista. Probablemente indique Pendiente en los encabezados de cuentas e indique el estado de la configuración de corrección automática. La creación de una política puede tardar varios minutos. Después de reemplazar el estado Pending (Pendiente) por recuentos de cuentas, puede elegir el nombre de la política para explorar el estado de cumplimiento de las cuentas y los recursos. Para obtener información, consulte Visualización de la información de cumplimiento de una AWS Firewall Manager política

Crear una AWS Firewall Manager política para Classic AWS WAF

Para crear una política de Firewall Manager para AWS WAF Classic (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/

fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

> **Note**
>
> Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Elija Crear política.
4. En Policy type (Tipo de política), seleccione AWS WAF Classic.
5. Si ya creó el grupo de reglas AWS WAF clásico que desea agregar a la política, elija Crear una AWS Firewall Manager política y agregar los grupos de reglas existentes. Si desea crear un nuevo grupo de reglas, elija Crear una política de Firewall Manager y agregar un nuevo grupo de reglas.
6. En Región, elija una Región de AWS. Para proteger CloudFront los recursos de Amazon, elige Global.

   Para proteger los recursos de varias regiones (distintas de CloudFront los recursos), debe crear políticas de Firewall Manager independientes para cada región.
7. Elija Siguiente.
8. Si está creando un grupo de reglas, siga las instrucciones de Creación de un grupo de reglas AWS WAF clásico. Después de crear el grupo de reglas, continúe con los pasos siguientes.
9. Escriba un nombre para la política.
10. Si agrega a un grupo de reglas existente, utilice el menú desplegable para seleccionar un grupo de reglas al que agregar y, a continuación, elija Add rule group (Agregar grupo de reglas).
11. Una política dispone de dos posibles acciones: Action set by rule group (Acción establecida por el grupo de reglas) y Count (Contar). Si desea probar la política y el grupo de reglas, establezca la acción en Count (Contar). Esta acción anula cualquier acción de bloqueo especificada por las reglas en el grupo de reglas. Es decir, si la acción de la política está establecida en Count (Contar), las solicitudes solo se contabilizan y no se bloquean. Por el contrario, si establece la acción de la política en Action set by rule group (Acción establecida por el grupo de reglas), se utilizan las acciones del grupo de reglas. Elija la acción apropiada.
12. Elija Siguiente.
13. En Cuentas de AWS a las que se aplica esta política, elija la opción de la siguiente manera:

- Si desea aplicar la política a todas las cuentas de su organización, deje la opción predeterminada, Incluir todas las cuentas de mi AWS organización.
- Si desea aplicar la política solo a cuentas específicas o a cuentas que se encuentran en unidades AWS Organizations organizativas (OU) específicas, elija Incluir solo las cuentas y unidades organizativas especificadas y, a continuación, agregue las cuentas y OU que desee incluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.
- Si desea aplicar la política a todas las cuentas o unidades AWS Organizations organizativas (OU) excepto a un conjunto específico, elija Excluir las cuentas y unidades organizativas especificadas e incluir todas las demás y, a continuación, agregue las cuentas y unidades organizativas que desee excluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.

Solo puede elegir una de las opciones.

Después de aplicar la política, Firewall Manager evalúa automáticamente las cuentas nuevas en función de la configuración. Por ejemplo, si solo incluye cuentas específicas, Firewall Manager no aplica la política a ninguna cuenta nueva. Como otro ejemplo, si incluye una unidad organizativa, cuando agrega una cuenta a la unidad organizativa o a cualquiera de sus unidades organizativas secundarias, Firewall Manager aplica automáticamente la política a la nueva cuenta.

14. Elija el tipo de recurso que desea proteger.
15. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

    Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

    Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.

16. Si desea aplicar automáticamente la política a los recursos existentes, elija Create and apply this policy to existing and new resources (Crear y aplicar esta política a los recursos nuevos y existentes).

    Esta opción crea una ACL web en cada cuenta aplicable de una organización de AWS y asocia la ACL web a los recursos en las cuentas. Esta opción también aplica la política a todos los nuevos recursos que coinciden con los criterios precedentes (tipo de recurso y etiquetas). Por otro lado, si elige Create policy but do not apply the policy to existing or new resources (Crear política pero no aplicarla a los recursos nuevos o existentes), Firewall Manager crea una ACL web en todas las cuentas de la organización que cumplen los requisitos necesarios, pero no la aplica a ningún recurso. Deberá aplicar la política a los recursos posteriormente. Elija la opción apropiada.
17. En Replace existing associated web ACLs (Sustituir ACL web asociadas existentes), puede elegir eliminar cualquier asociación ACL web que esté definida actualmente en los recursos dentro del ámbito y, a continuación, sustituirlos por asociaciones a las ACL web que crea con esta política. De forma predeterminada, Firewall Manager no elimina las asociaciones de ACL web existentes antes de agregar las nuevas. Si desea eliminar las existentes, seleccione esta opción.
18. Elija Siguiente.
19. Revise la nueva política. Para realizar cualquier cambio, elija Edit (Editar). Cuando esté satisfecho con la política, elija Create and apply policy (Crear y aplicar política).

Crear una AWS Firewall Manager política para AWS Shield Advanced

Creación de una política de Firewall Manager para Shield Advanced (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).

3. Elija Crear política.
4. Para Tipo de política, seleccione Shield Advanced.

   Para crear una política de Shield Advanced, debe estar suscrito a Shield Advanced. Se le pedirá que se suscriba si no lo ha hecho ya. Para obtener información sobre el coste de la suscripción, consulte Precios de AWS Shield Advanced.
5. En Región, elija una Región de AWS. Para proteger CloudFront las distribuciones de Amazon, elige Global.

   En las opciones de región que no sean Global, para proteger recursos en varias regiones, debe crear una política de Firewall Manager independiente para cada región.
6. Elija Siguiente.
7. En Nombre, introduzca un nombre descriptivo.
8. Solo para las políticas de región Global, puede elegir si desea administrar la mitigación automática de DDoS en la capa de aplicación de Shield Advanced. Para obtener información acerca de esta característica de Shield Advanced, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced.

   Puede elegir habilitar o deshabilitar la mitigación automática, o puede elegir ignorarla. Si decide ignorarla, Firewall Manager no administra en absoluto la mitigación automática de las protecciones Shield Advanced. Para obtener más información sobre estas opciones de la política, consulte Mitigación automática de DDoS en la capa de aplicación.
9. En Administración de ACL web, si desea que Firewall Manager administre las ACL web no asociadas, habilite Administrar ACL web no asociadas. Con esta opción, Firewall Manager crea ACL web en las cuentas dentro del alcance de la política solo si las ACL web serán utilizadas por al menos un recurso. Si en algún momento, una cuenta entra en el alcance de la política, Firewall Manager crea automáticamente una ACL web en la cuenta si al menos un recurso utilizará la ACL web. Al activar esta opción, el Firewall Manager realiza una limpieza única de las ACL web no asociadas de su cuenta. El proceso de limpieza puede tardar varias horas. Si un recurso sale del alcance de la política después de que el Firewall Manager haya creado una ACL web, el Firewall Manager no disociará el recurso de la ACL web. Para incluir la ACL web en la limpieza única, primero debe desasociar manualmente los recursos de la ACL web y, a continuación, activar la opción Administrar ACL web no asociadas.
10. En Acción de la política, se recomienda crear la política con la opción que no corrige automáticamente los recursos no compatibles. Al deshabilitar la solución automática, puede evaluar los efectos de la nueva política antes de aplicarla. Cuando esté seguro de que los

cambios son lo que desea, edite la política y cambie la acción de la política para habilitar la corrección automática.

Si, en su lugar, desea aplicar automáticamente la política a los recursos existentes dentro del ámbito, elija Auto remediate any noncompliant resources (Solucionar automáticamente los recursos no conformes). Esta opción aplica las protecciones Shield Advanced a cada cuenta aplicable de la AWS organización y a cada recurso aplicable de las cuentas.

Solo para las políticas de la región global, si elige Corregir automáticamente cualquier recurso que no cumpla con las normas, también puede optar por que Firewall Manager sustituya automáticamente cualquier asociación de ACL web AWS WAF clásica existente por nuevas asociaciones de ACL web que se hayan creado con la última versión de AWS WAF (v2). Si elige esta opción, Firewall Manager elimina las asociaciones con las ACL web de la versión anterior y crea nuevas asociaciones con las ACL web de la última versión, después de crear nuevas ACL web vacías en cualquier cuenta pertinente que aún no las tenga para la política. Para obtener más información acerca de esta opción, consulte Sustituya las ACL web AWS WAF clásicas por las ACL web de última versión.

11. Elija Siguiente.
12. En Cuentas de AWS a las que se aplica esta política, elija la opción de la siguiente manera:

    - Si desea aplicar la política a todas las cuentas de su organización, mantenga la selección predeterminada Incluir todas las cuentas de mi organización AWS .
    - Si desea aplicar la política solo a cuentas específicas o a cuentas que se encuentran en unidades AWS Organizations organizativas (OU) específicas, elija Incluir solo las cuentas y unidades organizativas especificadas y, a continuación, agregue las cuentas y las OU que desee incluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.
    - Si desea aplicar la política a todas las cuentas o unidades AWS Organizations organizativas (OU) excepto a un conjunto específico, elija Excluir las cuentas y unidades organizativas especificadas e incluir todas las demás y, a continuación, agregue las cuentas y unidades organizativas que desee excluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.

Solo puede elegir una de las opciones.

Después de aplicar la política, Firewall Manager evalúa automáticamente las cuentas nuevas en función de la configuración. Por ejemplo, si solo incluye cuentas específicas, Firewall Manager no aplica la política a ninguna cuenta nueva. Como otro ejemplo, si incluye una unidad organizativa, cuando agrega una cuenta a la unidad organizativa o a cualquiera de sus unidades organizativas secundarias, Firewall Manager aplica automáticamente la política a la nueva cuenta.

13. Elija el tipo de recurso que desea proteger.

    Firewall Manager no es compatible con Amazon Route 53 o AWS Global Accelerator. Si necesita utilizar Shield Advanced para proteger recursos de estos servicios, no puede utilizar una política de Firewall Manager. En su lugar, siga las instrucciones de Shield Advanced en Añadir AWS Shield Advanced protección a AWS los recursos.

14. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

    Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

    Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.

15. Elija Siguiente.

16. En el caso de las etiquetas de política, añada las etiquetas de identificación que desee añadir al recurso de políticas del Firewall Manager. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

17. Elija Siguiente.

18. Revise la nueva configuración de la política y vuelva a las páginas en las que necesite realizar algún ajuste.

    Cuando esté satisfecho con la política, elija Crear política. En el panel de políticas de AWS Firewall Manager , su política debe aparecer en la lista. Probablemente indique Pendiente en los encabezados de cuentas e indique el estado de la configuración de corrección automática. La

creación de una política puede tardar varios minutos. Después de reemplazar el estado Pending (Pendiente) por recuentos de cuentas, puede elegir el nombre de la política para explorar el estado de cumplimiento de las cuentas y los recursos. Para obtener información, consulte Visualización de la información de cumplimiento de una AWS Firewall Manager política

Crear una política de grupo de seguridad común de AWS Firewall Manager

Para obtener información sobre el funcionamiento de las políticas de grupos de seguridad comunes, consulte Políticas de grupos de seguridad comunes.

Para crear una política de grupo de seguridad común, debe tener un grupo de seguridad ya creado en la cuenta de administrador de Firewall Manager que desee utilizar como principal para la política. Puede administrar grupos de seguridad a través de Amazon Virtual Private Cloud (Amazon VPC) o Amazon Elastic Compute Cloud (Amazon EC2). Para obtener información, consulte Uso de grupos de seguridad en la Guía del usuario de Amazon VPC.

Para crear una política de grupo de seguridad común (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Elija Crear política.
4. En Policy type (Tipo de política), elija Security group (Grupo de seguridad).
5. En Security group policy type (Tipo de política de grupo de seguridad), elija Common security groups (Grupos de seguridad comunes).
6. En Región, elija una Región de AWS.
7. Elija Siguiente.
8. En Policy name (Nombre de la política), escriba un nombre fácil de recordar.
9. En Policy rules (Reglas de la política), haga lo siguiente:

a. En las opciones de reglas, elija las restricciones que desea aplicar a las reglas de grupo de seguridad y a los recursos que están dentro del ámbito de la política. Si elige Distribuir etiquetas del grupo de seguridad principal a los grupos de seguridad creados por esta política, también debe seleccionar Identificar e informar cuando los grupos de seguridad creados por esta política dejen de cumplir las reglas.

> **Important**
>
> Firewall Manager no distribuirá las etiquetas de sistema agregadas por AWS los servicios en los grupos de seguridad de réplica. Las etiquetas del sistema comienzan por el prefijo `aws:`. Además, Firewall Manager no actualizará las etiquetas de los grupos de seguridad existentes ni creará nuevos grupos de seguridad si la política tiene etiquetas que entren en conflicto con la política de etiquetas de la organización. Para obtener información sobre las políticas de etiquetas, consulte las políticas de etiquetas en la Guía del AWS Organizations usuario.

Si elige Distribuir las referencias a los grupos de seguridad del grupo de seguridad principal a los grupos de seguridad creados por esta política, Firewall Manager solo distribuirá las referencias a los grupos de seguridad si tienen una conexión de pares activa en Amazon VPC. Para obtener información acerca de esta opción, consulte Configuración de reglas de políticas.

b. Para los grupos de seguridad principales, elija Agregar grupos de seguridad y, a continuación, elija los grupos de seguridad que desee usar. Firewall Manager rellena la lista de grupos de seguridad de todas las instancias de Amazon VPC de la cuenta de administrador de Firewall Manager.

   De forma predeterminada, el número máximo de grupos de seguridad principales por política es de 3. Para obtener información sobre esta configuración, consulte AWS Firewall Manager cuotas.

c. En Policy action (Acción de la política), se recomienda crear la política sin la opción de corrección automática. Esto le permite evaluar los efectos de la nueva política antes de aplicarla. Cuando esté convencido de que los cambios son lo que desea, edite la política y cambie la acción de la política para habilitar la corrección automática de los recursos no conformes.

10. Elija Siguiente.
11. En Cuentas de AWS a las que se aplica esta política, elija la opción de la siguiente manera:

    - Si desea aplicar la política a todas las cuentas de su organización, deje la selección predeterminada, Incluir todas las cuentas de mi AWS organización.
    - Si desea aplicar la política solo a cuentas específicas o a cuentas que se encuentran en unidades AWS Organizations organizativas (OU) específicas, elija Incluir solo las cuentas y unidades organizativas especificadas y, a continuación, agregue las cuentas y OU que desee incluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.
    - Si desea aplicar la política a todas las cuentas o unidades AWS Organizations organizativas (OU) excepto a un conjunto específico, elija Excluir las cuentas y unidades organizativas especificadas e incluir todas las demás y, a continuación, agregue las cuentas y unidades organizativas que desee excluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.

    Solo puede elegir una de las opciones.

    Después de aplicar la política, Firewall Manager evalúa automáticamente las cuentas nuevas en función de la configuración. Por ejemplo, si solo incluye cuentas específicas, Firewall Manager no aplica la política a ninguna cuenta nueva. Como otro ejemplo, si incluye una unidad organizativa, cuando agrega una cuenta a la unidad organizativa o a cualquiera de sus unidades organizativas secundarias, Firewall Manager aplica automáticamente la política a la nueva cuenta.
12. En Resource type (Tipo de recurso), elija los tipos de recurso que desea proteger.

    Si elige Instancia EC2, puede elegir incluir todas las interfaces de red elásticas en cada instancia de Amazon EC2 o simplemente la interfaz predeterminada en cada instancia. Si tiene más de una interfaz de red elástica en cualquier instancia de Amazon EC2 dentro del ámbito, elegir la opción de incluir todas las interfaces permite a Firewall Manager aplicar la política a todas ellas. Cuando habilita la corrección automática, si Firewall Manager no puede aplicar la política a todas las interfaces de red elásticas de una instancia de Amazon EC2, la marca como no compatible.

13. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

    Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

    Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.
14. En el caso de recursos de VPC compartidos, si desea aplicar la política a los recursos de VPC compartidos, además de las VPC que poseen las cuentas, seleccione Incluir recursos de VPC compartidas.
15. Elija Siguiente.
16. Revise la configuración de la política para asegurarse de que es lo que desea y, a continuación, elija Create policy (Crear política).

Firewall Manager crea una réplica del grupo de seguridad principal en cada instancia de Amazon VPC contenida dentro de las cuentas pertinentes, hasta el límite máximo admitido de Amazon VPC por cuenta. Firewall Manager asocia los grupos de seguridad réplica a los recursos que están dentro del alcance de la política para cada cuenta pertinente. Para obtener más información sobre cómo funciona esta política, consulte Políticas de grupos de seguridad comunes.

Crear una política de grupo de seguridad de auditoría de contenido de AWS Firewall Manager

Para obtener información sobre el funcionamiento de las políticas de grupos de seguridad de auditoría de contenido, consulte Políticas de grupos de seguridad de auditoría de contenido.

Para algunas configuraciones de políticas de auditoría de contenido, debe proporcionar un grupo de seguridad de auditoría para que Firewall Manager lo utilice como plantilla. Por ejemplo, puede tener un grupo de seguridad de auditoría que contenga todas las reglas que no permite en ningún grupo de seguridad. Debe crear estos grupos de seguridad de auditoría con su cuenta de administrador de Firewall Manager para poder usarlos en su política. Puede administrar grupos de seguridad a través de Amazon Virtual Private Cloud (Amazon VPC) o Amazon Elastic Compute Cloud (Amazon EC2).

Para obtener información, consulte Uso de grupos de seguridad en la Guía del usuario de Amazon VPC.

Para crear una política de grupo de seguridad de auditoría de contenido (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Elija Crear política.
4. En Policy type (Tipo de política), elija Security group (Grupo de seguridad).
5. En Security group policy type (Tipo de política de grupo de seguridad), elija Auditing and enforcement of security group rules (Auditoría y aplicación de reglas de grupo de seguridad).
6. En Región, elija una Región de AWS.
7. Elija Siguiente.
8. En Policy name (Nombre de la política), escriba un nombre fácil de recordar.
9. En Reglas de política, elija la opción de reglas de política administradas o personalizadas que desee usar.

   a. En Configurar las reglas de políticas de auditoría administradas, haga lo siguiente:

      i. En Configurar las reglas de los grupos de seguridad para auditar, seleccione el tipo de reglas del grupo de seguridad al que desea que se aplique la política de auditoría.

      ii. Si desea realizar tareas como auditar las reglas en función de los protocolos, los puertos y la configuración del rango de CIDR de sus grupos de seguridad, seleccione Auditar las reglas de los grupos de seguridad excesivamente permisivas y seleccione las opciones que desee.

      Para hacer la selección de Regla que permite todo el tráfico, puede proporcionar una lista de aplicaciones personalizada para designar las aplicaciones que desea auditar.

Para obtener información sobre las listas de aplicaciones personalizadas y cómo utilizarlas en su política, consulte Listas administradas y Uso de listas administradas.

Para las selecciones que utilizan listas de protocolos, puede utilizar las listas existentes y crear listas nuevas. Para obtener información sobre las listas de protocolos y cómo utilizarlas en su política, consulte Listas administradas y Uso de listas administradas.

iii. Si desea auditar aplicaciones de alto riesgo en función de su acceso a rangos de CIDR reservados o no reservados, seleccione Auditar aplicaciones de alto riesgo y seleccione las opciones que desee.

Las siguientes selecciones se excluyen mutuamente: Aplicaciones que solo pueden acceder a rangos de CIDR reservados y Aplicaciones que pueden acceder a rangos de CIDR no reservados. Puede seleccionar como máximo una de ellas en cualquier política.

Para las selecciones que utilizan listas de aplicaciones, puede utilizar las listas existentes y crear listas nuevas. Para obtener información sobre las listas de aplicaciones y cómo utilizarlas en su política, consulte Listas administradas y Uso de listas administradas.

iv. Utilice la configuración de Anulaciones para anular de forma explícita otras configuraciones de la política. Puede optar por permitir siempre o denegar siempre reglas de grupos de seguridad específicos, independientemente de si cumplen con las demás opciones que haya establecido para la política.

Para esta opción, proporcione un grupo de seguridad de auditoría como plantilla de reglas permitidas o reglas rechazadas. Para los grupos de seguridad de auditoría, seleccione Agregar grupo de seguridad de auditoría y, a continuación, elija el grupo de seguridad que desea usar. Firewall Manager rellena la lista de grupos de seguridad de auditoría de todas las instancias de Amazon VPC de la cuenta de administrador de Firewall Manager. La cuota máxima predeterminada en el número de grupos de seguridad de auditoría para una política es uno. Para obtener información sobre cómo aumentar la cuota, consulte AWS Firewall Manager cuotas.

b. En Configurar reglas de política personalizadas, haga lo siguiente:

i. En las opciones de reglas, elija si desea permitir solo las reglas definidas en los grupos de seguridad de auditoría o denegar todas las reglas. Para obtener información sobre esta opción, consulte Políticas de grupos de seguridad de auditoría de contenido.

ii. Para los grupos de seguridad de auditoría, seleccione Agregar grupo de seguridad de auditoría y, a continuación, elija el grupo de seguridad que desea usar. Firewall Manager rellena la lista de grupos de seguridad de auditoría de todas las instancias de Amazon VPC de la cuenta de administrador de Firewall Manager. La cuota máxima predeterminada en el número de grupos de seguridad de auditoría para una política es uno. Para obtener información sobre cómo aumentar la cuota, consulte AWS Firewall Manager cuotas.

iii. En Policy action (Acción de la política), debe crear la política sin la opción de corrección automática. Esto le permite evaluar los efectos de la nueva política antes de aplicarla. Cuando esté convencido de que los cambios son lo que desea, edite la política y cambie la acción de la política para habilitar la corrección automática de los recursos no conformes.

10. Elija Siguiente.
11. En Cuentas de AWS a las que se aplica esta política, elija la opción de la siguiente manera:

    - Si desea aplicar la política a todas las cuentas de su organización, deje la selección predeterminada, Incluir todas las cuentas de mi AWS organización.
    - Si desea aplicar la política solo a cuentas específicas o a cuentas que se encuentran en unidades AWS Organizations organizativas (OU) específicas, elija Incluir solo las cuentas y unidades organizativas especificadas y, a continuación, agregue las cuentas y OU que desee incluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.
    - Si desea aplicar la política a todas las cuentas o unidades AWS Organizations organizativas (OU) excepto a un conjunto específico, elija Excluir las cuentas y unidades organizativas especificadas e incluir todas las demás y, a continuación, agregue las cuentas y unidades organizativas que desee excluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.

    Solo puede elegir una de las opciones.

    Después de aplicar la política, Firewall Manager evalúa automáticamente las cuentas nuevas en función de la configuración. Por ejemplo, si solo incluye cuentas específicas, Firewall Manager no aplica la política a ninguna cuenta nueva. Como otro ejemplo, si incluye una unidad

organizativa, cuando agrega una cuenta a la unidad organizativa o a cualquiera de sus unidades organizativas secundarias, Firewall Manager aplica automáticamente la política a la nueva cuenta.

12. En Resource type (Tipo de recurso), elija los tipos de recurso que desea proteger.
13. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

    Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

    Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.
14. Elija Siguiente.
15. Revise la configuración de la política para asegurarse de que es lo que desea y, a continuación, elija Create policy (Crear política).

Firewall Manager compara el grupo de seguridad de auditoría con los grupos de seguridad dentro del ámbito de la organización de AWS , según la configuración de las reglas de su política. Puede revisar el estado de la política en la consola AWS Firewall Manager de políticas. Una vez creada la política, puede editarla y habilitar la corrección automática para aplicar su política de grupo de seguridad de auditoría. Para obtener más información sobre cómo funciona esta política, consulte Políticas de grupos de seguridad de auditoría de contenido.

Crear una política de grupo de seguridad de auditoría de uso de AWS Firewall Manager

Para obtener información sobre el funcionamiento de las políticas de grupos de seguridad de auditoría de uso, consulte Políticas de grupos de seguridad de auditoría de uso.

Para crear una política de grupo de seguridad de auditoría de uso (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/

fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

> **Note**
>
> Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Elija Crear política.
4. En Policy type (Tipo de política), elija Security group (Grupo de seguridad).
5. En Tipo de política de grupo de seguridad, elija Auditoría y eliminación de grupos de seguridad redundantes y no asociados.
6. En Región, elija una Región de AWS.
7. Elija Siguiente.
8. En Policy name (Nombre de la política), escriba un nombre fácil de recordar.
9. En Policy rules (Reglas de la política), elija una o ambas opciones disponibles.

   - Si elige Los grupos de seguridad dentro del alcance de esta política deben ser utilizados por al menos un recurso, Firewall Manager elimina los grupos de seguridad que determine que no se utilizan. Cuando esta regla está habilitada, el Administrador de Firewall la ejecuta por última vez al guardar la política.

     Para obtener más información sobre cómo el Firewall Manager determina el uso y el momento de la corrección, consultePolíticas de grupos de seguridad de auditoría de uso.

     > **Note**
     >
     > Cuando utilice este tipo de política de auditoría de uso de los grupos de seguridad, evite realizar varios cambios en el estado de asociación de los grupos de seguridad incluidos en el ámbito de aplicación en un breve período de tiempo. Si lo hace, es posible que Firewall Manager pierda los eventos correspondientes.

     De forma predeterminada, Firewall Manager considera que los grupos de seguridad no cumplen con esta regla de política tan pronto como no se utilizan. Si lo desea, puede especificar un número de minutos que un grupo de seguridad puede permanecer sin utilizarse

antes de que se considere no conforme, hasta 525.600 minutos (365 días). Puede usar esta configuración para disponer de tiempo para asociar nuevos grupos de seguridad a los recursos.

> **Important**
>
> Si especifica un número de minutos distinto del valor predeterminado de cero, debe habilitar las relaciones indirectas AWS Config. De lo contrario, las políticas de los grupos de seguridad de auditoría de uso no funcionarán según lo previsto. Para obtener información sobre las relaciones indirectas en AWS Config, consulte Relaciones indirectas AWS Config en la Guía para AWS Config desarrolladores.

- Si elige Los grupos de seguridad dentro del alcance de esta política deben ser únicos, Firewall Manager consolida los grupos de seguridad redundantes, de modo que solo uno está asociado a los recursos. Si elige esta opción, Firewall Manager lo ejecuta en primer lugar cuando guarde la política.

10. En Policy action (Acción de la política), se recomienda crear la política sin la opción de corrección automática. Esto le permite evaluar los efectos de la nueva política antes de aplicarla. Cuando esté convencido de que los cambios son lo que desea, edite la política y cambie la acción de la política para habilitar la corrección automática de los recursos no conformes.
11. Elija Siguiente.
12. En Cuentas de AWS a las que se aplica esta política, elija la opción de la siguiente manera:

    - Si desea aplicar la política a todas las cuentas de su organización, deje la opción predeterminada, Incluir todas las cuentas de mi AWS organización.
    - Si desea aplicar la política solo a cuentas específicas o a cuentas que se encuentran en unidades AWS Organizations organizativas (OU) específicas, elija Incluir solo las cuentas y unidades organizativas especificadas y, a continuación, agregue las cuentas y OU que desee incluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.
    - Si desea aplicar la política a todas las cuentas o unidades AWS Organizations organizativas (OU) excepto a un conjunto específico, elija Excluir las cuentas y unidades organizativas especificadas e incluir todas las demás y, a continuación, agregue las cuentas y unidades organizativas que desee excluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas

secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.

Solo puede elegir una de las opciones.

Después de aplicar la política, Firewall Manager evalúa automáticamente las cuentas nuevas en función de la configuración. Por ejemplo, si solo incluye cuentas específicas, Firewall Manager no aplica la política a ninguna cuenta nueva. Como otro ejemplo, si incluye una unidad organizativa, cuando agrega una cuenta a la unidad organizativa o a cualquiera de sus unidades organizativas secundarias, Firewall Manager aplica automáticamente la política a la nueva cuenta.

13. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

    Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

    Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.
14. Elija Siguiente.
15. Si no ha excluido la cuenta de administrador de Firewall Manager del ámbito de la política, Firewall Manager le pedirá que lo haga. Al hacerlo, los grupos de seguridad de la cuenta de administrador de Firewall Manager que utiliza para políticas de grupos de seguridad comunes y de auditoría quedan bajo su control manual. Elija la opción que desee en este diálogo.
16. Revise la configuración de la política para asegurarse de que es lo que desea y, a continuación, elija Create policy (Crear política).

Si decide exigir grupos de seguridad únicos, Firewall Manager busca grupos de seguridad redundantes en cada instancia de Amazon VPC pertinente. A continuación, si decide exigir que cada grupo de seguridad sea utilizado por al menos un recurso, Firewall Manager busca grupos de seguridad que no se han utilizado durante los minutos especificados en la regla. Puede revisar el estado de la política en la consola AWS Firewall Manager de políticas. Para obtener más información sobre cómo funciona esta política, consulte Políticas de grupos de seguridad de auditoría de uso.

Crear una política AWS Firewall Manager de ACL de red

Para obtener información sobre cómo funcionan las políticas de ACL de red, consultePolíticas de ACL de red.

Para crear una política de ACL de red, debe saber cómo definir una ACL de red para usarla con las subredes de Amazon VPC. Para obtener más información, consulte Controlar el tráfico a las subredes mediante ACL de red y Trabajar con ACL de red en la Guía del usuario de Amazon VPC.

Para crear una política de ACL de red (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Elija Crear política.
4. Para el tipo de política, elija Network ACL.
5. En Región, elija una Región de AWS.
6. Elija Siguiente.
7. En Nombre de política, introduzca un nombre descriptivo.
8. En el caso de las reglas de política, defina las reglas que desee que se ejecuten siempre en las ACL de red que Firewall Manager administra por usted. Las ACL de red supervisan y gestionan el tráfico entrante y saliente, por lo que en su política debe definir las reglas para ambas direcciones.

   En cualquier dirección, se definen las reglas que se deben ejecutar siempre primero y las que se deben ejecutar siempre en último lugar. En las ACL de red que administra Firewall Manager, los propietarios de las cuentas pueden definir reglas personalizadas para que se ejecuten entre la primera y la última regla.

9. Para la acción de política, si desea identificar las subredes y las ACL de red que no cumplen con las normas, pero no tomar ninguna medida correctiva todavía, elija Identificar los recursos que no cumplen con las reglas de la política, pero que no se corrigen automáticamente. Puede cambiar estas opciones más adelante.

   Si, por el contrario, desea aplicar la política automáticamente a las subredes existentes dentro del ámbito de aplicación, seleccione Corregir automáticamente cualquier recurso que no cumpla con las normas. Con esta opción, también especifica si se debe forzar la corrección cuando el comportamiento de las reglas de política en materia de gestión del tráfico entre en conflicto con las reglas personalizadas que se encuentran en la ACL de la red. Independientemente de si fuerza o no una corrección, Firewall Manager informa de normas contradictorias en sus infracciones de conformidad.

10. Elija Siguiente.

11. En Cuentas de AWS a las que se aplica esta política, elija la opción de la siguiente manera:

    - Si desea aplicar la política a todas las cuentas de su organización, deje la opción predeterminada, Incluir todas las cuentas de mi AWS organización.
    - Si desea aplicar la política solo a cuentas específicas o a cuentas que se encuentran en unidades AWS Organizations organizativas (OU) específicas, elija Incluir solo las cuentas y unidades organizativas especificadas y, a continuación, agregue las cuentas y OU que desee incluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.
    - Si desea aplicar la política a todas las cuentas o unidades AWS Organizations organizativas (OU) excepto a un conjunto específico, elija Excluir las cuentas y unidades organizativas especificadas e incluir todas las demás y, a continuación, agregue las cuentas y unidades organizativas que desee excluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.

    Solo puede elegir una de las opciones.

    Después de aplicar la política, Firewall Manager evalúa automáticamente las cuentas nuevas en función de la configuración. Por ejemplo, si incluye solo cuentas específicas, el Firewall Manager no aplicará la política a ninguna cuenta nueva o diferente. Como otro ejemplo, si incluye una

unidad organizativa, cuando agrega una cuenta a la unidad organizativa o a cualquiera de sus unidades organizativas secundarias, Firewall Manager aplica automáticamente la política a la nueva cuenta.

12. Para el tipo de recurso, la configuración se fija en Subredes.
13. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

    Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

    Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.
14. Elija Siguiente.
15. Revise la configuración de la política para asegurarse de que es lo que desea y, a continuación, elija Create policy (Crear política).

Firewall Manager crea la política y comienza a monitorear y administrar las ACL de la red incluidas en el ámbito de aplicación de acuerdo con su configuración. Para obtener más información sobre cómo funciona esta política, consulte Políticas de ACL de red.

Crear una AWS Firewall Manager política para AWS Network Firewall

En una política de Firewall Manager Network Firewall, se utilizan los grupos de reglas que se administran en AWS Network Firewall. Para obtener información sobre cómo administrar sus grupos de reglas, consulte Grupos de reglas de AWS Network Firewall en la Guía para desarrolladores de Network Firewall.

Para obtener información acerca de las políticas de Firewall Manager Network Firewall, consulte AWS Network Firewall políticas.

Para crear una política de Firewall Manager para AWS Network Firewall (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/

fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

> **Note**
>
> Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Elija Crear política.
4. Para Policy type (Tipo de política), seleccione AWS Network Firewall.
5. En Tipo de administración del firewall, elija cómo desea que Firewall Manager administre los firewalls de la política. Puede elegir entre las siguientes opciones:

   - Distribuido: Firewall Manager crea y mantiene puntos de conexión de firewall en cada VPC que se encuentra dentro del alcance de la política.
   - Centralizado: Firewall Manager crea y mantiene los puntos de conexión en una única VPC de inspección.
   - Importar firewalls existentes: Firewall Manager importa los firewalls existentes desde Network Firewall mediante conjuntos de recursos. Para obtener información acerca de los conjuntos de recursos, consulte Trabajar con conjuntos de recursos en Firewall Manager.
6. En Región, elija una Región de AWS. Para proteger los recursos en varias regiones, debe crear políticas distintas para cada región.
7. Elija Siguiente.
8. En Nombre de política, introduzca un nombre descriptivo. Firewall Manager incluye el nombre de la política en los nombres de los firewalls de Network Firewall y las políticas de firewall que crea.
9. En la política de configuración de AWS Network Firewall , configure la política de firewall como lo haría en Network Firewall. Agregue sus grupos de reglas sin estado y con estado y especifique las acciones predeterminadas de la política. Si lo desea, puede establecer el orden de evaluación de las reglas con estado de la política y las acciones predeterminadas, así como la configuración de registro. Para obtener información sobre la administración de políticas de firewall de Network Firewall, consulte Políticas de firewall AWS Network Firewall en la Guía para desarrolladores de AWS Network Firewall .

   Al crear la política de firewall de red de Firewall Manager Network Firewall, Firewall Manager crea políticas de firewall para las cuentas que están dentro del alcance. Los administradores de

cuentas individuales pueden agregar grupos de reglas a las políticas de firewall, pero no pueden cambiar la configuración que proporciona aquí.

10. Elija Siguiente.
11. Realice una de las siguientes acciones, en función del tipo de administración de firewall que haya seleccionado en el paso anterior:

    - Si utiliza un tipo de administración de firewall distribuido, en Configuración de puntos de conexión de AWS Firewall Manager , en Ubicación del punto de conexión del firewall, seleccione una de las siguientes opciones:
      - Configuración de punto de conexión personalizada: Firewall Manager crea firewalls para cada VPC dentro del alcance de la política, en las zonas de disponibilidad que especifique. Cada firewall contiene como mínimo un punto de conexión de firewall.
        - En Zonas de disponibilidad, seleccione en qué zonas de disponibilidad desea crear los puntos de conexión del firewall. Puede seleccionar las zonas de disponibilidad por Nombre de la zona de disponibilidad o por ID de la zona de disponibilidad.
        - Si desea proporcionar los bloques CIDR para que Firewall Manager los utilice en las subredes de firewall de sus VPC, todos deben ser bloques CIDR de /28. Ingrese un bloque por línea. Si las omite, Firewall Manager elegirá por usted las direcciones IP entre las que están disponibles en las VPC.

        > **Note**
        >
        > La corrección automática se realiza automáticamente para las políticas de AWS Firewall Manager Network Firewall, por lo que aquí no verá ninguna opción para elegir no realizar la corrección automática.

      - Configuración automática de puntos de conexión: Firewall Manager crea automáticamente puntos de conexión de firewall en las zonas de disponibilidad con subredes públicas en su VPC.
        - Para la configuración de los puntos de conexión del firewall, especifique cómo desea que Firewall Manager administre los puntos de conexión del firewall. Se recomienda utilizar varios puntos de conexión para una alta disponibilidad.
    - Si utiliza un tipo de administración de firewall centralizada, en la configuración de punto de conexión de AWS Firewall Manager , en Configuración de VPC de inspección, introduzca el ID de cuenta de AWS del propietario de la VPC de inspección y el ID de la VPC de inspección.

- En Zonas de disponibilidad, seleccione en qué zonas de disponibilidad desea crear los puntos de conexión del firewall. Puede seleccionar las zonas de disponibilidad por Nombre de la zona de disponibilidad o por ID de la zona de disponibilidad.
- Si desea proporcionar los bloques CIDR para que Firewall Manager los utilice en las subredes de firewall de sus VPC, todos deben ser bloques CIDR de /28. Ingrese un bloque por línea. Si las omite, Firewall Manager elegirá por usted las direcciones IP entre las que están disponibles en las VPC.

> **Note**
>
> La corrección automática se realiza automáticamente para las políticas de AWS Firewall Manager Network Firewall, por lo que aquí no verá ninguna opción para elegir no realizar la corrección automática.

- Si está utilizando un tipo de administración de firewalls de importación de firewalls existentes, en Conjuntos de recursos, agregue uno o más conjuntos de recursos. Un conjunto de recursos define los firewalls existentes de Network Firewall que pertenecen a la cuenta de su organización y que desea administrar de forma centralizada en esta política. Para añadir un conjunto de recursos a la política, primero debe crear un conjunto de recursos mediante la consola o la PutResourceSetAPI. Para obtener información acerca de los conjuntos de recursos, consulte Trabajar con conjuntos de recursos en Firewall Manager. Para obtener más información sobre la importación de firewalls existentes desde Network Firewall, consulte Importar firewalls existentes.

12. Elija Siguiente.
13. Si su política utiliza un tipo de administración de firewall distribuido, en Administración de rutas, elija si Firewall Manager supervisará y alertará sobre el tráfico que debe enrutarse a través de los puntos de conexión de firewall respectivos.

> **Note**
>
> Si selecciona Supervisar, no podrá cambiar la configuración a Desactivado más adelante. La supervisión continúa hasta que elimine la política.

14. Para Tipo de tráfico, si lo desea, añada los puntos de conexión del tráfico por los que desee enrutar el tráfico para inspeccionar el firewall.

15. En el caso de Permitir el tráfico entre zonas de disponibilidad obligatorio, si habilita esta opción, Firewall Manager considerará compatible el enrutamiento que envía tráfico fuera de una Zona de Disponibilidad para su inspección, en las Zonas de Disponibilidad que no tienen su propio punto de conexión de firewall. Las zonas de disponibilidad que tienen puntos de conexión siempre deben inspeccionar su propio tráfico.
16. Elija Siguiente.
17. Para Alcance de la política, en esta política se aplica a Cuentas de AWS , elija la opción siguiente:

    - Si desea aplicar la política a todas las cuentas de su organización, deje la selección predeterminada, Incluir todas las cuentas de mi AWS organización.
    - Si desea aplicar la política solo a cuentas específicas o a cuentas que se encuentran en unidades AWS Organizations organizativas (OU) específicas, elija Incluir solo las cuentas y unidades organizativas especificadas y, a continuación, agregue las cuentas y OU que desee incluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.
    - Si desea aplicar la política a todas las cuentas o unidades AWS Organizations organizativas (OU) excepto a un conjunto específico, elija Excluir las cuentas y unidades organizativas especificadas e incluir todas las demás y, a continuación, agregue las cuentas y unidades organizativas que desee excluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.

    Solo puede elegir una de las opciones.

    Después de aplicar la política, Firewall Manager evalúa automáticamente las cuentas nuevas en función de la configuración. Por ejemplo, si solo incluye cuentas específicas, Firewall Manager no aplica la política a ninguna cuenta nueva. Como otro ejemplo, si incluye una unidad organizativa, cuando agrega una cuenta a la unidad organizativa o a cualquiera de sus unidades organizativas secundarias, Firewall Manager aplica automáticamente la política a la nueva cuenta.
18. El Tipo de recurso para las políticas de Network Firewall es VPC.
19. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la

inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.

20. Elija Siguiente.
21. En el caso de las etiquetas de política, añada las etiquetas de identificación que desee añadir al recurso de políticas del Firewall Manager. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.
22. Elija Siguiente.
23. Revise la nueva configuración de la política y vuelva a las páginas en las que necesite realizar algún ajuste.

    Cuando esté satisfecho con la política, elija Crear política. En el panel de políticas de AWS Firewall Manager , su política debe aparecer en la lista. Probablemente indique Pendiente en los encabezados de cuentas e indique el estado de la configuración de corrección automática. La creación de una política puede tardar varios minutos. Después de reemplazar el estado Pending (Pendiente) por recuentos de cuentas, puede elegir el nombre de la política para explorar el estado de cumplimiento de las cuentas y los recursos. Para obtener información, consulte Visualización de la información de cumplimiento de una AWS Firewall Manager política

Creación de una AWS Firewall Manager política para Amazon Route 53 Resolver DNS Firewall

En una política de DNS Firewall de Firewall Manager, utilice grupos de reglas que administra en Amazon Route 53 Resolver DNS Firewall. Para obtener información sobre la administración de sus grupos de reglas, consulte Cómo administrar grupos de reglas y reglas en DNS Firewall en la Guía para desarrolladores de Amazon Route 53.

Para obtener información acerca de las políticas de Firewall Manager DNS Firewall, consulte Políticas de DNS firewall de Amazon Route 53 Resolver.

Creación de una política de Firewall Manager para Amazon Route 53 Resolver DNS Firewall (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Elija Crear política.
4. En Tipo de política, seleccione Amazon Route 53 Resolver DNS Firewall.
5. En Región, elija una Región de AWS. Para proteger los recursos en varias regiones, debe crear políticas distintas para cada región.
6. Elija Siguiente.
7. En Nombre de política, introduzca un nombre descriptivo.
8. En la configuración de políticas, agregue los grupos de reglas que desee que DNS Firewall evalúe lo primero y último entre las asociaciones de grupos de reglas de sus VPC. Puede añadir hasta dos grupos de reglas a la política.

   Al crear la política de DNS Firewall DNS en Firewall Manager, Firewall Manager crea las asociaciones de grupos de reglas, con las prioridades de asociación que haya proporcionado, para las VPC y las cuentas que están dentro del alcance. Los administradores de cuentas individuales pueden añadir asociaciones de grupos de reglas entre la primera y la última asociación, pero no pueden cambiar las asociaciones que defina aquí. Para obtener más información, consulte Políticas de DNS firewall de Amazon Route 53 Resolver.
9. Seleccione Siguiente.
10. En Cuentas de AWS a las que se aplica esta política, elija la opción de la siguiente manera:

    - Si desea aplicar la política a todas las cuentas de su organización, deje la selección predeterminada, Incluir todas las cuentas de mi AWS organización.

- Si desea aplicar la política solo a cuentas específicas o a cuentas que se encuentran en unidades AWS Organizations organizativas (OU) específicas, elija Incluir solo las cuentas y unidades organizativas especificadas y, a continuación, agregue las cuentas y OU que desee incluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.
- Si desea aplicar la política a todas las cuentas o unidades AWS Organizations organizativas (OU) excepto a un conjunto específico, elija Excluir las cuentas y unidades organizativas especificadas e incluir todas las demás y, a continuación, agregue las cuentas y unidades organizativas que desee excluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.

Solo puede elegir una de las opciones.

Después de aplicar la política, Firewall Manager evalúa automáticamente las cuentas nuevas en función de la configuración. Por ejemplo, si solo incluye cuentas específicas, Firewall Manager no aplica la política a ninguna cuenta nueva. Como otro ejemplo, si incluye una unidad organizativa, cuando agrega una cuenta a la unidad organizativa o a cualquiera de sus unidades organizativas secundarias, Firewall Manager aplica automáticamente la política a la nueva cuenta.

11. El Tipo de recurso para las políticas de DNS Firewall es VPC.
12. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

    Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

    Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.
13. Elija Siguiente.

14. En el caso de las etiquetas de política, añada las etiquetas de identificación que desee añadir al recurso de políticas del Firewall Manager. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.
15. Elija Siguiente.
16. Revise la nueva configuración de la política y vuelva a las páginas en las que necesite realizar algún ajuste.

    Cuando esté satisfecho con la política, elija Crear política. En el panel de políticas de AWS Firewall Manager , su política debe aparecer en la lista. Probablemente indique Pendiente en los encabezados de cuentas e indique el estado de la configuración de corrección automática. La creación de una política puede tardar varios minutos. Después de reemplazar el estado Pending (Pendiente) por recuentos de cuentas, puede elegir el nombre de la política para explorar el estado de cumplimiento de las cuentas y los recursos. Para obtener información, consulte Visualización de la información de cumplimiento de una AWS Firewall Manager política

Creación de una AWS Firewall Manager política para el NGFW en la nube de Palo Alto Networks

Con una política de Firewall Manager para el Firewall de próxima generación en la nube de Palo Alto Networks (Palo Alto Networks Cloud NGFW), puede utilizar Firewall Manager para implementar los recursos de NGFW en la nube de Palo Alto Networks y administrar las pilas de NGFW de forma centralizada en todas sus cuentas. AWS

Para obtener información sobre políticas de NGFW en la nube de Palo Alto Networks de Firewall Manager, consulte Políticas de NGFW en la nube de Palo Alto Networks. Para obtener información sobre cómo configurar y administrar NGFW en la nube de Palo Alto Networks para Firewall Manager, consulte la documentación de NGFW en la nube de Palo Alto Networks en AWS.

Requisitos previos

Existen varios pasos obligatorios para preparar su cuenta de AWS Firewall Manager. Estos pasos se describen en AWS Firewall Manager requisitos previos. Complete todos los requisitos previos antes de continuar con el siguiente paso.

Creación de una política de Firewall Manager para NGFW en la nube de Palo Alto Networks (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Elija Crear política.
4. Para el tipo de política, elija Palo Alto Networks Cloud NGFW. Si aún no te has suscrito al servicio NGFW en la nube de Palo Alto Networks en AWS Marketplace, tendrás que hacerlo primero. Para suscribirte en AWS Marketplace, selecciona Ver detalles del AWS Marketplace.
5. Para Modelo de implementación, elija Modelo distribuido o Modelo centralizado. El modelo de implementación determina la forma en que Firewall Manager administra los puntos de conexión de la política. Con el modelo distribuido, Firewall Manager mantiene los puntos de conexión del firewall en cada VPC que se encuentre dentro del ámbito de aplicación de la política. Con el modelo centralizado, Firewall Manager mantiene un único punto de conexión en una VPC de inspección.
6. En Región, selecciona una Región de AWS. Para proteger los recursos en varias regiones, debe crear políticas distintas para cada región.
7. Elija Siguiente.
8. En Nombre de política, introduzca un nombre descriptivo.
9. En la configuración de la política, elija la política de firewall de NGFW en la nube de Palo Alto Networks para asociarla a esta política. La lista de políticas de firewall de NGFW en la nube de Palo Alto Networks contiene todas las políticas de firewall de NGFW en la nube de Palo Alto Networks asociadas a su inquilino de NGFW en la nube de Palo Alto Networks. Para obtener información sobre cómo crear y administrar las políticas de firewall de NGFW en la nube de Palo Alto Networks, consulte la guía Implemente el NGFW en la nube de Palo Alto Networks, que incluye el AWS Firewall Manager tema en la AWS guía de implementación del NGFW en la nube de Palo Alto Networks. AWS

10. Para el registro de NGFW en Palo Alto Networks Cloud (opcional), elija los tipos de registro de NGFW de Palo Alto Networks Cloud que desee registrar para su política. Para obtener información sobre los tipos de registro del NGFW en la nube de Palo Alto Networks, consulte Configurar el registro del NGFW en la nube de Palo Alto Networks en la guía de implementación del NGFW AWS en la nube de Palo Alto Networks. AWS

    En Destino del registro, especifique en qué momento Firewall Manager debe escribir los registros.

11. Elija Siguiente.

12. En Configurar punto de conexión de firewall de terceros, lleve a cabo una de las siguientes acciones, en función de si utiliza el modelo de implementación distribuido o centralizado para crear los puntos de conexión de firewall:

    - Si utiliza el modelo de implementación distribuida para esta política, en Zonas de disponibilidad, seleccione en qué zonas de disponibilidad desea crear los puntos de conexión del firewall. Puede seleccionar las zonas de disponibilidad por Nombre de la zona de disponibilidad o por ID de la zona de disponibilidad.
    - Si utiliza el modelo de implementación centralizada para esta política, en Configuración de punto de conexión de AWS Firewall Manager de Configuración de VPC de inspección, introduzca el ID de cuenta de AWS del propietario de la VPC de inspección y el ID de VPC de la VPC de inspección.
        - En Zonas de disponibilidad, seleccione en qué zonas de disponibilidad desea crear los puntos de conexión del firewall. Puede seleccionar las zonas de disponibilidad por Nombre de la zona de disponibilidad o por ID de la zona de disponibilidad.

13. Si desea proporcionar los bloques CIDR para que Firewall Manager los utilice en las subredes de firewall de sus VPC, todos deben ser bloques CIDR de /28. Ingrese un bloque por línea. Si las omite, Firewall Manager elegirá por usted las direcciones IP entre las que están disponibles en las VPC.

    > **Note**
    >
    > La corrección automática se realiza automáticamente para las políticas de AWS Firewall Manager Network Firewall, por lo que aquí no verá ninguna opción para elegir no realizar la corrección automática.

14. Elija Siguiente.

15. Para Alcance de la política, en esta política se aplica a Cuentas de AWS , elija la opción siguiente:

    - Si desea aplicar la política a todas las cuentas de su organización, deje la opción predeterminada, Incluir todas las cuentas de mi AWS organización.
    - Si desea aplicar la política solo a cuentas específicas o a cuentas que se encuentran en unidades AWS Organizations organizativas (OU) específicas, elija Incluir solo las cuentas y unidades organizativas especificadas y, a continuación, agregue las cuentas y OU que desee incluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.
    - Si desea aplicar la política a todas las cuentas o unidades AWS Organizations organizativas (OU) excepto a un conjunto específico, elija Excluir las cuentas y unidades organizativas especificadas e incluir todas las demás y, a continuación, agregue las cuentas y unidades organizativas que desee excluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.

    Solo puede elegir una de las opciones.

    Después de aplicar la política, Firewall Manager evalúa automáticamente las cuentas nuevas en función de la configuración. Por ejemplo, si solo incluye cuentas específicas, Firewall Manager no aplica la política a ninguna cuenta nueva. Como otro ejemplo, si incluye una unidad organizativa, cuando agrega una cuenta a la unidad organizativa o a cualquiera de sus unidades organizativas secundarias, Firewall Manager aplica automáticamente la política a la nueva cuenta.
16. El Tipo de recurso para las políticas de Network Firewall es VPC.
17. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

    Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.

18. En Conceder acceso entre cuentas, seleccione Descargar plantilla de AWS CloudFormation . Esto descarga una AWS CloudFormation plantilla que puedes usar para crear una AWS CloudFormation pila. Esta pila crea un AWS Identity and Access Management rol que otorga permisos entre cuentas a Firewall Manager para administrar los recursos de NGFW en la nube de Palo Alto Networks. Para obtener información acerca de las pilas, consulte Uso de pilas en la Guía del usuario de AWS CloudFormation .
19. Elija Siguiente.
20. En el caso de las etiquetas de política, añada las etiquetas de identificación que desee añadir al recurso de políticas del Firewall Manager. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.
21. Elija Siguiente.
22. Revise la nueva configuración de la política y vuelva a las páginas en las que necesite realizar algún ajuste.

    Cuando esté satisfecho con la política, elija Crear política. En el panel de políticas de AWS Firewall Manager , su política debe aparecer en la lista. Probablemente indique Pendiente en los encabezados de cuentas e indique el estado de la configuración de corrección automática. La creación de una política puede tardar varios minutos. Después de reemplazar el estado Pending (Pendiente) por recuentos de cuentas, puede elegir el nombre de la política para explorar el estado de cumplimiento de las cuentas y los recursos. Para obtener información, consulte Visualización de la información de cumplimiento de una AWS Firewall Manager política

Crear una AWS Firewall Manager política para Fortigate Cloud Native Firewall (CNF) como servicio

Con una política de Firewall Manager para Fortigate CNF, puede usar Firewall Manager para implementar y administrar los recursos de Fortigate CNF en todas sus cuentas. AWS

Para obtener información acerca de las políticas de Firewall Manager Fortigate CNF, consulte Políticas de Fortigate Cloud Native Firewall (CNF) como servicio. Para obtener información sobre cómo configurar Fortigate CNF para su uso con Firewall Manager, consulte la documentación de Fortinet.

Requisitos previos

Existen varios pasos obligatorios para preparar su cuenta de AWS Firewall Manager. Estos pasos se describen en AWS Firewall Manager requisitos previos. Complete todos los requisitos previos antes de continuar con el siguiente paso.

Creación de una política de Firewall Manager para Fortigate CNF (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Elija Crear política.
4. Para Tipo de política, seleccione Fortigate Cloud Native Firewall (CNF) como servicio. Si aún no se ha suscrito al servicio Fortigate CNF en el AWS Marketplace, primero tendrá que hacerlo. Para suscribirte en AWS Marketplace, selecciona Ver detalles del AWS Marketplace.
5. Para Modelo de implementación, elija Modelo distribuido o Modelo centralizado. El modelo de implementación determina la forma en que Firewall Manager administra los puntos de conexión de la política. Con el modelo distribuido, Firewall Manager mantiene los puntos de conexión del firewall en cada VPC que se encuentre dentro del ámbito de aplicación de la política. Con el modelo centralizado, Firewall Manager mantiene un único punto de conexión en una VPC de inspección.
6. En Región, selecciona una Región de AWS. Para proteger los recursos en varias regiones, debe crear políticas distintas para cada región.
7. Elija Siguiente.
8. En Nombre de política, introduzca un nombre descriptivo.
9. En la configuración de la política, elija la política de firewall Fortigate CNF para asociarla a esta política. La lista de políticas de firewall de Fortigate CNF contiene todas las políticas de firewall de Fortigate CNF asociadas a su inquilino de Fortigate CNF. Para obtener información sobre cómo crear y administrar clientes de Fortigate CNF, consulte la documentación de Fortinet.

10. Elija Siguiente.
11. En Configurar punto de conexión de firewall de terceros, lleve a cabo una de las siguientes acciones, en función de si utiliza el modelo de implementación distribuido o centralizado para crear los puntos de conexión de firewall:

    - Si utiliza el modelo de implementación distribuida para esta política, en Zonas de disponibilidad, seleccione en qué zonas de disponibilidad desea crear los puntos de conexión del firewall. Puede seleccionar las zonas de disponibilidad por Nombre de la zona de disponibilidad o por ID de la zona de disponibilidad.
    - Si utiliza el modelo de implementación centralizada para esta política, en Configuración de punto de conexión de AWS Firewall Manager de Configuración de VPC de inspección, introduzca el ID de cuenta de AWS del propietario de la VPC de inspección y el ID de VPC de la VPC de inspección.
        - En Zonas de disponibilidad, seleccione en qué zonas de disponibilidad desea crear los puntos de conexión del firewall. Puede seleccionar las zonas de disponibilidad por Nombre de la zona de disponibilidad o por ID de la zona de disponibilidad.
12. Si desea proporcionar los bloques CIDR para que Firewall Manager los utilice en las subredes de firewall de sus VPC, todos deben ser bloques CIDR de /28. Ingrese un bloque por línea. Si las omite, Firewall Manager elegirá por usted las direcciones IP entre las que están disponibles en las VPC.

    > **Note**
    >
    > La corrección automática se realiza automáticamente para las políticas de AWS Firewall Manager Network Firewall, por lo que aquí no verá ninguna opción para elegir no realizar la corrección automática.

13. Elija Siguiente.
14. Para Alcance de la política, en esta política se aplica a Cuentas de AWS , elija la opción siguiente:

    - Si desea aplicar la política a todas las cuentas de su organización, deje la opción predeterminada, Incluir todas las cuentas de mi AWS organización.
    - Si desea aplicar la política solo a cuentas específicas o a cuentas que se encuentran en unidades AWS Organizations organizativas (OU) específicas, elija Incluir solo las cuentas y unidades organizativas especificadas y, a continuación, agregue las cuentas y OU que desee

incluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.

- Si desea aplicar la política a todas las cuentas o unidades AWS Organizations organizativas (OU) excepto a un conjunto específico, elija Excluir las cuentas y unidades organizativas especificadas e incluir todas las demás y, a continuación, agregue las cuentas y unidades organizativas que desee excluir. Especificar una unidad organizativa equivale a especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.

Solo puede elegir una de las opciones.

Después de aplicar la política, Firewall Manager evalúa automáticamente las cuentas nuevas en función de la configuración. Por ejemplo, si solo incluye cuentas específicas, Firewall Manager no aplica la política a ninguna cuenta nueva. Como otro ejemplo, si incluye una unidad organizativa, cuando agrega una cuenta a la unidad organizativa o a cualquiera de sus unidades organizativas secundarias, Firewall Manager aplica automáticamente la política a la nueva cuenta.

15. El Tipo de recurso para las políticas de Network Firewall es VPC.
16. En el caso de los recursos, puede limitar el alcance de la política mediante el etiquetado, ya sea incluyendo o excluyendo los recursos con las etiquetas que especifique. Puede utilizar la inclusión o la exclusión, y no ambas. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.

    Si especifica más de una etiqueta, un recurso debe tener todas las etiquetas que se van a incluir o excluir.

    Las etiquetas de recursos solo pueden tener valores que no sean nulos. Si omite el valor de una etiqueta, el Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.
17. En Conceder acceso entre cuentas, seleccione Descargar plantilla de AWS CloudFormation . Esto descarga una AWS CloudFormation plantilla que puedes usar para crear una AWS CloudFormation pila. Esta pila crea un AWS Identity and Access Management rol que otorga permisos multicuenta al Administrador de Firewall para administrar los recursos de Fortigate CNF. Para obtener información acerca de las pilas, consulte Uso de pilas en la Guía del usuario

de AWS CloudFormation . Para crear una pila, necesitará el ID de cuenta del portal de Fortigate CNF.

18. Elija Siguiente.
19. En el caso de las etiquetas de política, añada las etiquetas de identificación que desee añadir al recurso de políticas del Firewall Manager. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.
20. Elija Siguiente.
21. Revise la nueva configuración de la política y vuelva a las páginas en las que necesite realizar algún ajuste.

    Cuando esté satisfecho con la política, elija Crear política. En el panel de políticas de AWS Firewall Manager , su política debe aparecer en la lista. Probablemente indique Pendiente en los encabezados de cuentas e indique el estado de la configuración de corrección automática. La creación de una política puede tardar varios minutos. Después de reemplazar el estado Pending (Pendiente) por recuentos de cuentas, puede elegir el nombre de la política para explorar el estado de cumplimiento de las cuentas y los recursos. Para obtener información, consulte Visualización de la información de cumplimiento de una AWS Firewall Manager política

Eliminar una AWS Firewall Manager política

Puede eliminar una política de Firewall Manager realizando los pasos que se describen a continuación.

Para eliminar una política (consola)

1. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
2. Elija la opción situada junto a la política que desea eliminar.
3. Elija Eliminar.

> **Note**
>
> Cuando elimine una política de grupo de seguridad común de Firewall Manager, para quitar los grupos de seguridad de réplica de la política, elija la opción de eliminar los recursos creados por la política. De lo contrario, después de eliminar el principal, las réplicas permanecen y requerirán administración manual en cada instancia de Amazon VPC.

> **Important**
>
> Cuando elimina una política de Firewall Manager Shield Advanced, la política se elimina, pero sus cuentas permanecen suscritas a Shield Advanced.

AWS Firewall Manager alcance de la política

El alcance de la política define dónde se aplica la política. Puede aplicar políticas controladas de forma centralizada a todas las cuentas y recursos de la AWS Organizations organización o a un subconjunto de ellas. Para obtener instrucciones sobre cómo establecer el alcance de la política, consulte Creación de una AWS Firewall Manager política.

Opciones de alcance de la política en AWS Firewall Manager

Cuando agrega una nueva cuenta o recurso a su organización, Firewall Manager lo evalúa automáticamente en función de su configuración para cada política y aplica la política en función de esta configuración. Por ejemplo, puede optar por aplicar una política a todas las cuentas excepto a los números de cuenta de una lista específica; también puede optar por aplicar una política solo a los recursos que tengan todas las etiquetas de una lista.

Cuentas de AWS dentro del alcance

La configuración que proporcione para definir a los Cuentas de AWS afectados por la política determinará a qué cuentas de su AWS organización se aplicará la política. Puede optar por aplicar la política de una de las siguientes maneras:

- A todas las cuentas de la organización
- Solo para una lista concreta de números de cuenta incluidos y unidades organizativas (OU) de AWS Organizations
- Para todos excepto una lista específica de números de cuenta excluidos y unidades organizativas (OU) de AWS Organizations

Para obtener información al respecto AWS Organizations, consulte la Guía AWS Organizations del usuario.

Recursos en el ámbito

De manera similar a la configuración para las cuentas dentro del alcance, la configuración que proporcione para los recursos determina a qué tipos de recursos dentro del alcance se aplicará la política. Puede elegir una de las siguientes opciones:

- Todos los recursos
- Recursos que tienen todas las etiquetas que especifique
- Todos los recursos excepto aquellos que tienen todas las etiquetas que especifique

Solo puede especificar etiquetas de recursos con valores que no sean nulos. Si no proporciona nada para el valor, Firewall Manager guarda la etiqueta con un valor de cadena vacío: «». Las etiquetas de recursos solo coinciden con las etiquetas que tienen la misma clave y el mismo valor.

Para obtener más información sobre cómo etiquetar los recursos, consulte Uso de Tag Editor.

Gestión del alcance de la política en AWS Firewall Manager

Cuando existen políticas, Firewall Manager las administra continuamente y las aplica a los recursos nuevos Cuentas de AWS y a los recursos a medida que se agregan, de acuerdo con el alcance de la política.

Cómo administra Cuentas de AWS y utiliza Firewall Manager sus recursos

Si una cuenta o un recurso queda fuera del ámbito de aplicación por cualquier motivo, AWS Firewall Manager no elimina automáticamente las protecciones ni elimina los recursos administrados por Firewall Manager a menos que active la casilla Eliminar automáticamente las protecciones de los recursos que salen del ámbito de la política.

> **Note**
>
> La opción Eliminar automáticamente las protecciones de los recursos que quedan fuera del ámbito de aplicación de la política no está disponible para las AWS Shield Advanced políticas AWS WAF clásicas.

Al seleccionar esta casilla de verificación, AWS Firewall Manager se limpiarán automáticamente los recursos que el Firewall Manager administra para las cuentas cuando esas cuentas salen del ámbito de la política. Por ejemplo, Firewall Manager desasociará una ACL web administrada por Firewall Manager de un recurso protegido del cliente cuando este abandone el alcance de la política.

Para determinar qué recursos deben ser eliminados de la protección cuando un recurso del cliente esta fuera del alcance de la política, Firewall Manager sigue estas pautas:

- Comportamiento predeterminado:
  - Se eliminan las reglas AWS Config administradas asociadas. Este comportamiento es independiente de la casilla de verificación.
  - Se eliminan todas las listas de control de acceso AWS WAF web (ACL web) asociadas que no contengan ningún recurso. Este comportamiento es independiente de la casilla de verificación.
  - Cualquier recurso protegido que quede fuera del alcance permanece asociado y protegido. Por ejemplo, un Application Load Balancer (Equilibrador de carga de aplicación) o una API de API Gateway que esté asociada a una ACL web permanece asociada a la ACL web y la protección permanece vigente.
- Con la casilla Eliminar automáticamente las protecciones de los recursos que salen del alcance de la política seleccionada:
  - Se eliminan las reglas AWS Config administradas asociadas. Este comportamiento es independiente de la casilla de verificación.
  - Se eliminan todas las listas de control de acceso AWS WAF web (ACL web) asociadas que no contengan ningún recurso. Este comportamiento es independiente de la casilla de verificación.
  - Cualquier recurso protegido que quede fuera del ámbito de aplicación se disocia automáticamente y se elimina de la protección del Firewall Manager cuando abandona el ámbito de la política. Por ejemplo, en el caso de una política de grupo de seguridad, un acelerador de Elastic Inference o una instancia de Amazon EC2 se disocian automáticamente del grupo de seguridad replicado cuando abandona el ámbito de la política. El grupo de seguridad replicado y sus recursos se eliminan automáticamente de la protección.

Listas administradas

Las listas administradas de aplicaciones y protocolos simplifican la configuración y la administración de las políticas de los grupos de seguridad de auditoría de contenido de AWS Firewall Manager . Las listas administradas se utilizan para definir los protocolos y las aplicaciones que su política permite y no permite. Para obtener información sobre las políticas de grupo de seguridad de auditoría de contenido, consulte Políticas de grupos de seguridad de auditoría de contenido.

Puede utilizar los siguientes tipos de listas administradas en una política de grupo de seguridad de auditoría de contenido:

- Listas de aplicaciones y listas de protocolos de Firewall Manager: Firewall Manager administra estas listas.
  - Las listas de aplicaciones incluyen `FMS-Default-Public-Access-Apps-Allowed` y `FMS-Default-Public-Access-Apps-Denied`, las cuales describen las aplicaciones de uso común que deberían permitirse o denegarse al público en general.
  - Las listas de protocolos incluyen `FMS-Default-Protocols-Allowed`, una lista de protocolos de uso común que deberían estar permitidos al público en general. Puede usar cualquier lista administrada por Firewall Manager, pero no puede editarla ni eliminarla.
- Listas de aplicaciones y listas de protocolos personalizadas: usted administra estas listas. Puede crear listas de cualquier tipo con la configuración que necesite. Tiene el control total sobre sus propias listas de administración personalizada y puede crearlas, editarlas y eliminarlas según sea necesario.

> **Note**
>
> Actualmente, Firewall Manager no comprueba las referencias a una lista de administración personalizada al eliminarla. Esto significa que puede eliminar una lista de aplicaciones o una lista de protocolos de administración personalizada incluso cuando una política activa la esté utilizando. Esto puede provocar que la política deje de funcionar. Elimine una lista de aplicaciones o una lista de protocolos solo después de comprobar que ninguna política activa hace referencia a ella.

Las listas administradas son AWS recursos. Puede etiquetar una lista de administración personalizada. No puede etiquetar una lista administrada por Firewall Manager.

Control de versiones de listas administradas

Las listas de administración personalizada no tienen versiones. Al editar una lista personalizada, las políticas que hacen referencia a la lista utilizan automáticamente la lista actualizada.

Las listas administradas por Firewall Manager tienen control de versiones. El equipo del servicio Firewall Manager publica nuevas versiones según sea necesario para aplicar las prácticas recomendadas de seguridad a las listas.

Cuando utiliza una lista administrada por Firewall Manager en una política, elige la estrategia de control de versiones de la siguiente manera:

- Última versión disponible: si no especifica una configuración de versión explícita para la lista, la política utilizará automáticamente la última versión. Esta es la única opción disponible a través de la consola.
- Versión explícita: si especifica una versión para la lista, su política utilizará esa versión. La política permanece bloqueada en la versión que ha especificado hasta que modifique la configuración de la versión. Para especificar la versión, debe definir la política fuera de la consola, por ejemplo, mediante la CLI o uno de los SDK.

Para obtener más información sobre cómo elegir la configuración de versión para una lista, consulte Uso de listas administradas en las políticas de los grupos de seguridad de auditoría de contenido.

Uso de listas administradas en las políticas de los grupos de seguridad de auditoría de contenido

Cuando cree una política de grupo de seguridad de auditoría de contenido, puede optar por utilizar reglas de política de auditoría administrada. Algunas de las configuraciones de esta opción requieren una lista de aplicaciones administrada o una lista de protocolos administrada. Algunos ejemplos de estas configuraciones son los protocolos permitidos en las reglas de los grupos de seguridad y las aplicaciones que pueden acceder a Internet.

Se aplican las siguientes restricciones a cada configuración de política que utilice una lista administrada:

- Puede especificar como máximo una lista administrada por Firewall Manager para cualquier configuración. De forma predeterminada, puede especificar como máximo una lista personalizada. El límite de la listas personalizadas es flexible, por lo que puede solicitar un aumento de la misma. Para obtener más información, consulte AWS Firewall Manager cuotas.
- En la consola, si selecciona una lista administrada por Firewall Manager, no podrá especificar la versión. La política siempre utilizará la última versión de la lista. Para especificar la versión, debe definir la política fuera de la consola, por ejemplo, mediante la CLI o uno de los SDK. Para obtener información sobre el control de versiones de las listas administradas por Firewall Manager, consulte Control de versiones de listas administradas.

Para obtener información acerca de cómo crear una política de grupo de seguridad de auditoría de contenido a través de la consola, consulte Crear una política de grupo de seguridad de auditoría de contenido.

Creación de una lista de aplicaciones de administración personalizada

Creación de una nueva lista de aplicaciones de administración personalizada

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Listas de aplicaciones.
3. En la página Listas de aplicaciones, seleccione Crear lista de aplicación.
4. En la página Crear lista de aplicación, asigne un nombre a la lista. No utilice el prefijo `fms-`, ya que está reservado para Firewall Manager.
5. Especifique una aplicación ya sea proporcionando el protocolo y el número de puerto, o seleccionando una aplicación del menú desplegable Tipo. Asigne un nombre a la especificación de su aplicación.
6. Seleccione Agregar otro según sea necesario y complete la información de la solicitud hasta que haya completado su lista.
7. (Opcional) Aplique etiquetas a su lista.
8. Seleccione Guardar para guardar la lista y volver a la página de Listas de aplicaciones.

Creación de una lista de protocolos de administración personalizada

Creación de una lista de protocolos de administración personalizada

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

> **Note**
>
> Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Listas de protocolos.
3. En la página de listas de protocolos, seleccione Crear lista de protocolos.
4. En la página de creación de listas de protocolos, asigne un nombre a su lista. No utilice el prefijo `fms-`, ya que está reservado para Firewall Manager.
5. Especifique un protocolo.
6. Seleccione Agregar otro según sea necesario y complete la información del protocolo hasta que haya completado su lista.
7. (Opcional) Aplique etiquetas a su lista.
8. Seleccione Guardar para guardar su lista y volver a la página de Listas de aplicaciones.

Visualización de una lista administrada

Cómo ver una lista de aplicaciones o una lista de protocolos

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Listas de aplicaciones o Listas de protocolos.

   La página muestra todas las listas del tipo seleccionado que están disponibles para su uso. Las listas que administra Firewall Manager tienen una Y en la ManagedListcolumna.

3. Para ver los detalles de una lista, elija el nombre. La página de detalles muestra el contenido de la lista y cualquier etiqueta.

En el caso de las listas administradas por Firewall Manager, también puede ver las versiones disponibles seleccionando el menú desplegable Versión.

Eliminación de una lista de administración personalizada

Puede eliminar listas de administración personalizada. No puede editar ni eliminar listas administradas por Firewall Manager.

> **Note**
>
> Actualmente, Firewall Manager no comprueba las referencias a una lista de administración personalizada al eliminarla. Esto significa que puede eliminar una lista de aplicaciones o una lista de protocolos de administración personalizada incluso cuando una política activa la esté utilizando. Esto puede provocar que la política deje de funcionar. Solo elimine una lista de aplicaciones o una lista de protocolos después de comprobar que ninguna política activa hace referencia a ella.

Eliminación de una lista de protocolos o aplicaciones de administración personalizada

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. Asegúrese de que la lista que desea eliminar no esté en uso en ninguna de las políticas de su grupo de seguridad de auditoría de la siguiente manera:

   a. En el panel de navegación, seleccione Security policies (Políticas de seguridad).

   b. En la página de políticas de AWS Firewall Manager , seleccione y edite sus grupos de seguridad de auditoría y elimine cualquier referencia a la lista personalizada que desee eliminar.

Si elimina una lista de administración personalizada que esté en uso en una política de auditoría de un grupo de seguridad, la política que la utiliza puede dejar de funcionar.

3. En el panel de navegación, seleccione Listas de aplicaciones o Listas de protocolos, según el tipo de lista que desee eliminar.
4. En la página de listas, seleccione la lista personalizada que desea eliminar y seleccione Eliminar.

AWS WAF políticas

En una AWS WAF política de Firewall Manager, se especifican los grupos de AWS WAF reglas que se quieren usar en todos los recursos. Al aplicar la política, Firewall Manager crea ACL web en las cuentas dentro del alcance de la política, según cómo configure la administración de las ACL web en su política. En las ACL web creadas por la política, los administradores de cuentas individuales pueden agregar reglas y grupos de reglas, además de los grupos de reglas que haya definido mediante Firewall Manager.

Cómo administra Firewall Manager las ACL web

Firewall Manager crea ACL web en función de cómo configure la opción Administrar ACL web no asociadas en su política o de la `optimizeUnassociatedWebACL` configuración del tipo de SecurityServicePolicyDatadatos de la API.

Si habilita la administración de ACL web no asociadas, Firewall Manager crea ACL web en las cuentas dentro del alcance de la política solo si las ACL web van a ser utilizadas al menos por un recurso. Si en algún momento, una cuenta entra en el alcance de la política, Firewall Manager crea automáticamente una ACL web en la cuenta si al menos un recurso utilizará la ACL web. Cuando habilita la administración de ACL web no asociadas, Firewall Manager realiza una limpieza única de las ACL web no asociadas de su cuenta. Durante la limpieza, Firewall Manager omite cualquier ACL web que haya modificado después de su creación, por ejemplo, si agregó un grupo de reglas a la ACL web o modificó sus configuraciones. El proceso de limpieza puede tardar varias horas. Si un recurso sale del alcance de la política después de que el Firewall Manager haya creado una ACL web, el Firewall Manager disociará el recurso de la ACL web, pero no realizará la limpieza de la ACL web no asociada. Firewall Manager solo realiza la limpieza de las ACL web no asociadas cuando se habilita por primera vez la administración de las ACL web no asociadas en una política.

Si no habilita esta opción, Firewall Manager no administrará las ACL web no asociadas y el Firewall Manager creará automáticamente una ACL web en cada cuenta que esté dentro del alcance de la política.

Muestreo y métricas CloudWatch

AWS Firewall Manager permite el muestreo y CloudWatch las métricas de Amazon para las ACL web y los grupos de reglas que crea para una AWS WAF política.

Estructura de nomenclatura de ACL web

Cuando Firewall Manager crea una ACL web para la política, le asigna el nombre `FMManagedWebACLV2-`*`policy name`*`-`*`timestamp`* a la ACL web. La marca de tiempo está en milisegundos UTC. Por ejemplo, `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`.

> **Note**
>
> Si un recurso configurado con la mitigación automática avanzada de DDoS en la capa de aplicación entra en el ámbito de aplicación de una AWS WAF política, Firewall Manager no podrá asociar la ACL web creada por la AWS WAF política al recurso.

Grupos de reglas en las políticas AWS WAF

Las ACL web administradas por las AWS WAF políticas del Firewall Manager contienen tres conjuntos de reglas. Estos conjuntos proporcionan un nivel más alto de priorización para las reglas y grupos de reglas en la ACL web:

- Primeros grupos de reglas, definidos por usted en la AWS WAF política del Firewall Manager. AWS WAF evalúa primero estos grupos de reglas.
- Reglas y grupos de reglas definidos por los administradores de cuentas en las ACL web. AWS WAF evalúa las reglas o grupos de reglas siguientes administrados por la cuenta.
- Últimos grupos de reglas, definidos por usted en la AWS WAF política del Firewall Manager. AWS WAF evalúa estos grupos de reglas en último lugar.

Dentro de cada uno de estos conjuntos de reglas, AWS WAF evalúa las reglas y los grupos de reglas como de costumbre, según su configuración de prioridad dentro del conjunto.

En el primer y último conjunto de grupos de reglas de la política, solo puede agregar grupos de reglas. Puedes usar grupos de reglas gestionados, que las reglas AWS gestionadas y AWS Marketplace los vendedores crean y mantienen por ti. También puede administrar y usar sus propios grupos de reglas. Para obtener más información acerca de todas estas opciones, consulte AWS WAF grupos de reglas.

Si desea utilizar sus propios grupos de reglas, créelos antes de crear su política de Firewall Manager de AWS WAF . Para obtener instrucciones, consulte Administrar sus propios grupos de reglas. Para utilizar una regla personalizada individual, debe definir su propio grupo de reglas, definir la regla dentro de él y, a continuación, utilizar el grupo de reglas en la política.

El primer y el último grupo de AWS WAF reglas que administra a través del Firewall Manager tienen nombres que comienzan con `PREFMManaged-` o`POSTFMManaged-`, respectivamente, seguidos del nombre de la política del Administrador de Firewall y la marca de tiempo de creación del grupo de reglas, en milisegundos UTC. Por ejemplo, `PREFMManaged-MyWAFPolicyName-1621880555123`.

Para obtener información sobre cómo se AWS WAF evalúan las solicitudes web, consulte. Evaluación de reglas y grupos de reglas de ACL web

Para obtener información sobre el procedimiento para crear una AWS WAF política de Firewall Manager, consulteCrear una AWS Firewall Manager política para AWS WAF.

Firewall Manager permite el muestreo y CloudWatch las métricas de Amazon para los grupos de reglas que defina para la AWS WAF política.

Los propietarios de las cuentas individuales tienen el control total sobre las métricas y la configuración del muestreo de cualquier regla o grupo de reglas que agreguen a las ACL web administradas de la política.

Configurar el registro para una AWS WAF política

Puede habilitar el registro centralizado de sus AWS WAF políticas para obtener información detallada sobre el tráfico que analiza su ACL web en su organización. La información de los registros incluye la hora en que se AWS WAF recibió la solicitud de tu AWS recurso, información detallada sobre la solicitud y las medidas adoptadas para cumplir la regla de que todas las cuentas incluidas en el ámbito de aplicación coincidieron con cada solicitud. Puede enviar sus registros a una transmisión de datos de Amazon Data Firehose o a un depósito de Amazon Simple Storage Service (S3). Para obtener información sobre el AWS WAF registro, consulte Registro del tráfico de ACL AWS WAF web la Guía para AWS WAF desarrolladores.

> **Note**
>
> AWS Firewall Manager admite esta opción para la versión clásica AWS WAFV2, no para la AWS WAF versión clásica.

Temas

Destinos de registro

En esta sección se describen los destinos de registro que puede elegir para enviar los registros AWS WAF de sus políticas. Cada sección proporciona instrucciones a fin de configurar el registro para el tipo de destino e información sobre cualquier comportamiento específico del tipo de destino. Una vez que haya configurado el destino de registro, puede proporcionar sus especificaciones a la AWS WAF política de Firewall Manager para empezar a iniciar sesión en él.

Firewall Manager no puede ver los errores de registro después de crear la configuración de registro. Es su responsabilidad comprobar que la entrega de registros funciona según lo previsto.

> **Note**
>
> Firewall Manager no modifica ninguna configuración de registro existente en las cuentas de los miembros de su organización.

Temas

Flujos de datos de Amazon Data Firehose

En este tema se proporciona información para enviar los registros de tráfico de ACL web a una transmisión de datos de Amazon Data Firehose.

Cuando habilitas el registro de Amazon Data Firehose, Firewall Manager envía los registros de las ACL web de tu política a una Amazon Data Firehose donde has configurado un destino de almacenamiento. Tras habilitar el registro, AWS WAF entrega los registros de cada ACL web configurada, a través del punto de enlace HTTPS de Kinesis Data Firehose, al destino de almacenamiento configurado. Antes de usarla, pruebe la transmisión de entrega para asegurarse de que tiene el rendimiento suficiente para alojar los registros de su organización. Para obtener más información sobre cómo crear una Amazon Kinesis Data Firehose y revisar los registros almacenados, consulte ¿Qué es Amazon Data Firehose?

Debe tener los siguientes permisos para habilitar correctamente el registro con Kinesis:

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

Al configurar un destino de registro de Amazon Data Firehose en una AWS WAF política, Firewall Manager crea una ACL web para la política en la cuenta de administrador de Firewall Manager de la siguiente manera:

- Firewall Manager crea la ACL web en la cuenta de administrador de Firewall Manager, independientemente de si la cuenta está dentro del alcance de la política.
- La ACL web tiene el registro activado, con un nombre de registro `FMManagedWebACLV2-Logging`*`policy name`*`-`*`timestamp`*, donde la marca de tiempo es la hora UTC en la que se habilitó el registro para la ACL web, en milisegundos. Por ejemplo, `FMManagedWebACLV2-LoggingMyWAFPolicyName-1621880565180`. La ACL web no tiene grupos de reglas ni recursos asociados.
- Se le cobrará por la ACL web de acuerdo con las pautas AWS WAF de precios. Para obtener más información, consulte AWS WAF Precios.
- Firewall Manager elimina la ACL web cuando usted elimina la política.

Para obtener información acerca de los roles vinculados a servicios y el permiso `iam:CreateServiceLinkedRole`, consulte Uso de roles vinculados a servicios para AWS WAF.

Para obtener más información sobre cómo crear tu flujo de entrega, consulta Cómo crear un flujo de entrega de Amazon Data Firehose.

Buckets de Amazon Simple Storage Service Batch

En este tema se proporciona información para enviar los registros de tráfico de ACL web a un bucket de Amazon S3.

El bucket que elija como destino de registro debe ser propiedad de una cuenta de administrador de Firewall Manager. Para obtener información sobre los requisitos para crear su bucket de Amazon S3 para los requisitos de registro y denominación de los buckets, consulte Amazon Simple Storage Service en la Guía para desarrolladores de AWS WAF .

Consistencia final

Cuando realiza cambios en AWS WAF las políticas configuradas con un destino de registro de Amazon S3, Firewall Manager actualiza la política del bucket para añadir los permisos necesarios para el registro. Al hacerlo, Firewall Manager sigue los modelos de last-writer-wins semántica y coherencia de datos que sigue Amazon Simple Storage Service. Si realiza simultáneamente varias actualizaciones de políticas en un destino de Amazon S3 en la consola de Firewall Manager o mediante la PutPolicyAPI, es posible que algunos permisos no se guarden. Para obtener más información acerca del modelo de coherencia de Amazon S3, consulte Modelo de coherencia de datos de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Permisos para publicar registros en un bucket de Amazon S3

La configuración del registro de tráfico de ACL web para un bucket de Amazon S3 en una AWS WAF política requiere los siguientes ajustes de permisos. Firewall Manager adjunta automáticamente estos permisos a su bucket de Amazon S3 cuando usted configura Amazon S3 como su destino de registro para dar permiso al servicio para publicar registros en el bucket. Si desea administrar un acceso más detallado a sus recursos de registro y del Firewall Manager, puede configurar estos permisos. Para obtener información sobre la administración de permisos, consulte Administración de acceso a recursos de AWS en la Guía del usuario de IAM. Para obtener información sobre las políticas AWS WAF administradas, consulteAWS políticas gestionadas para AWS WAF.

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryForFirewallManager",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheckFMS",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
```

```
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-DOC-EXAMPLE-BUCKET"
        },
        {
            "Sid": "AWSLogDeliveryWriteFMS",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/policy-id/
AWSLogs/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

Para evitar el problema de escalonamiento de privilegios entre servicios, puede agregar las claves de contexto de condición global `aws:SourceArn` y `aws:SourceAccount` a la política de su bucket. Para agregar estas claves, puede modificar la política que el Firewall Manager crea para usted al configurar el destino del registro o, si desea un control detallado, puede crear su propia política. Si agrega estas condiciones a su política de destino de registro, Firewall Manager no validará ni supervisará la protección de escalonamiento de privilegios. Para obtener información general sobre el problema del suplente confuso, consulte El problema del escalonamiento de privilegios en la Guía del usuario de IAM.

Cuando agregue `sourceAccount`, agregue las propiedades `sourceArn`, aumentará el tamaño de la política del bucket. Si va a agregar una lista larga de propiedades `sourceArn` agregue `sourceAccount`, procure no superar el límite de tamaño de la política de bucket de Amazon S3.

En el siguiente ejemplo se muestra cómo evitar el problema del suplente confuso mediante el uso de las claves de contexto de condición global `aws:SourceArn` y `aws:SourceAccount` en la política de su bucket. *`member-account-id`*Sustitúyalos por los ID de cuenta de los miembros de tu organización.

```
{
```

```
    "Version":"2012-10-17",
    "Id":"AWSLogDeliveryForFirewallManager",
    "Statement":[
       {
          "Sid":"AWSLogDeliveryAclCheckFMS",
          "Effect":"Allow",
          "Principal":{
             "Service":"delivery.logs.amazonaws.com"
          },
          "Action":"s3:GetBucketAcl",
          "Resource":"arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
          "Condition":{
             "StringEquals":{
                "aws:SourceAccount":[
                   "member-account-id",
                   "member-account-id"
                ]
             },
             "ArnLike":{
                "aws:SourceArn":[
                   "arn:aws:logs:*:member-account-id:*",
                   "arn:aws:logs:*:member-account-id:*"
                ]
             }
          }
       },
       {
          "Sid":"AWSLogDeliveryWriteFMS",
          "Effect":"Allow",
          "Principal":{
             "Service":"delivery.logs.amazonaws.com"
          },
          "Action":"s3:PutObject",
          "Resource":"arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/policy-id/AWSLogs/*",
          "Condition":{
             "StringEquals":{
                "s3:x-amz-acl":"bucket-owner-full-control",
                "aws:SourceAccount":[
                     "member-account-id",
                   "member-account-id"
                ]
             },
             "ArnLike":{
                "aws:SourceArn":[
```

```
                "arn:aws:logs:*:member-account-id-1:*",
                "arn:aws:logs:*:member-account-id-2:*"
            ]
        }
    }
  }
]
}
```

Uso de cifrado del servidor del bucket de Amazon S3

Puede activar el cifrado del lado del servidor de Amazon S3 o utilizar una clave gestionada por el AWS Key Management Service cliente en su bucket de S3. Si eliges usar el cifrado predeterminado de Amazon S3 en tu bucket de Amazon S3 para AWS WAF los registros, no necesitas realizar ninguna acción especial. Sin embargo, si decide utilizar una clave de cifrado proporcionada por el cliente para cifrar sus datos en reposo de Amazon S3, debe añadir la siguiente declaración de permiso a su AWS Key Management Service política de claves:

```
{
            "Sid": "Allow Logs Delivery to use the key",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
}
```

Para obtener información sobre el uso de claves de cifrado proporcionadas por el cliente con Amazon S3, consulte Uso del cifrado del servidor con claves proporcionadas por el cliente (SSE-C) en la Guía del usuario de Amazon Simple Storage Service.

Habilitación de registros

El siguiente procedimiento describe cómo habilitar el registro de una AWS WAF política en la consola de Firewall Manager.

Para habilitar el registro de una AWS WAF política

1. Para poder habilitar el registro, debe configurar los recursos de destino del registro de la siguiente manera:

   - Amazon Kinesis Data Streams: cree una Amazon Data Firehose con su cuenta de administrador de Firewall Manager. Utilice un nombre que empiece por el prefijo `aws-waf-logs-`. Por ejemplo, `aws-waf-logs-firewall-manager-central`. Cree la instancia de Data Firehose con un origen PUT y en la región en la que opera. Si vas a capturar troncos para Amazon CloudFront, crea la manguera de incendios en EE. UU. Este (Norte de Virginia). Antes de usarla, pruebe la transmisión de entrega para asegurarse de que tiene el rendimiento suficiente para alojar los registros de su organización. Para obtener más información, consulte Creación de un flujo de entrega de Amazon Data Firehose.
   - Buckets de Amazon Simple Storage Service: cree un bucket de Amazon S3 de acuerdo con las directrices del tema Amazon Simple Storage Service en la Guía para desarrolladores de AWS WAF . También debe configurar su bucket de Amazon S3 con los permisos que se indican en Permisos para publicar registros en un bucket de Amazon S3 .
2. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

3. En el panel de navegación, seleccione Políticas de Seguridad.
4. Elija la AWS WAF política para la que desee habilitar el registro. Para obtener más información acerca del registro en AWS WAF , consulte Registro del tráfico de ACL AWS WAF web.
5. En la pestaña Detalles de la política, en la sección Reglas de la política, seleccione Editar.
6. Para la configuración del registro, seleccione Habilitar el registro para activar el registro. El registro ofrece obtener información detallada sobre el tráfico que analiza su ACL web. Seleccione el destino del registro y, a continuación, seleccione el destino del registro que haya configurado. Debe elegir un destino de registro cuyo nombre comience con `aws-waf-logs-`. Para obtener información sobre la configuración de un destino de AWS WAF registro, consulteConfigurar el registro para una AWS WAF política.

7. (Opcional) Si no desea determinados campos y sus valores incluidos en los registros, redacte esos campos. Elija el campo que se va a redactar y, a continuación, elija Add (Añadir). Repita según sea necesario para redactar campos adicionales. Los campos redactados aparecen como `REDACTED` en los registros. Por ejemplo, si redacta el campo URI, el campo URI de los registros será `REDACTED`.
8. (Opcional) Si no desea enviar todas las solicitudes a los registros, agregue sus criterios de filtrado y su comportamiento. En Filtrar registros, para cada filtro que desee aplicar, elija Agregar filtro y, a continuación, elija sus criterios de filtrado y especifique si desea conservar o eliminar las solicitudes que coincidan con los criterios. Cuando termine de agregar los filtros, si es necesario, modifique el comportamiento de registro predeterminado. Para obtener más información, consulte Configuración de registro de ACL web en la Guía para desarrolladores de AWS WAF .
9. Elija Siguiente.
10. Revise su configuración y, a continuación, seleccione Guardar para guardar los cambios en la política.

Deshabilitar los registros

El siguiente procedimiento describe cómo deshabilitar el registro de una AWS WAF política en la consola de Firewall Manager.

Para deshabilitar el registro de una AWS WAF política

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Políticas de Seguridad.
3. Elija la AWS WAF política para la que desee deshabilitar el registro.
4. En la pestaña Detalles de la política, en la sección Reglas de la política, seleccione Editar.
5. En Estado de configuración de registro, seleccione Desactivado.

6. Elija Siguiente.
7. Revise su configuración y, a continuación, seleccione Guardar para guardar los cambios en la política.

AWS Shield Advanced políticas

En una AWS Shield política de Firewall Manager, usted elige los recursos que desea proteger. Al aplicar la política con la corrección automática habilitada, para cada recurso del ámbito que aún no esté asociado a una ACL AWS WAF web, Firewall Manager asocia una ACL AWS WAF web vacía. La ACL web vacía se utiliza para la supervisión de Shield. Si, a continuación, asocia cualquier otra ACL web al recurso, Firewall Manager elimina la asociación ACL web vacía.

> **Note**
>
> Cuando un recurso que está dentro del ámbito de una AWS WAF política entra en el ámbito de una política Shield Advanced configurada con una mitigación automática de DDoS en la capa de aplicación, Firewall Manager aplica la protección Shield Advanced solo después de asociar la ACL web creada por la AWS WAF política.

Cómo se AWS Firewall Manager gestionan las ACL web no asociadas en las políticas Shield

Puede configurar si el Firewall Manager administra las ACL web no asociadas por usted mediante la configuración Administrar las ACL web no asociadas de su política o mediante la `optimizeUnassociatedWebACLs` configuración del tipo de SecurityServicePolicyDatadatos de la API. Si habilita la administración de ACL web no asociadas en su política, Firewall Manager crea ACL web en las cuentas dentro del alcance de la política solo si las ACL web van a ser utilizadas al menos por un recurso. Si en algún momento, una cuenta entra en el alcance de la política, Firewall Manager crea automáticamente una ACL web en la cuenta si al menos un recurso utilizará la ACL web.

Cuando habilita la administración de ACL web no asociadas, Firewall Manager realiza una limpieza única de las ACL web no asociadas de su cuenta. El proceso de limpieza puede tardar varias horas. Si un recurso sale del alcance de la política después de que el Firewall Manager haya creado una ACL web, el Firewall Manager no disocia el recurso de la ACL web. Si desea que Firewall

Manager limpie la ACL web, primero debe desasociar manualmente los recursos de la ACL web y, a continuación, habilitar la opción de administrar ACL web no asociadas en su política.

Si no habilita esta opción, Firewall Manager no administrará las ACL web no asociadas y el Firewall Manager creará automáticamente una ACL web en cada cuenta que esté dentro del alcance de la política.

Cómo AWS Firewall Manager gestiona los cambios de alcance en las políticas de Shield

Las cuentas y los recursos pueden quedar fuera del ámbito de aplicación de una política de AWS Firewall Manager Shield Advanced debido a una serie de cambios, como cambios en la configuración del ámbito de la política, cambios en las etiquetas de un recurso y la eliminación de una cuenta de una organización. Para obtener información general sobre la configuración del alcance de la política, consulte AWS Firewall Manager alcance de la política.

Con una política de AWS Firewall Manager Shield Advanced, si una cuenta o un recurso queda fuera del alcance, Firewall Manager deja de supervisar la cuenta o el recurso.

Si una cuenta queda fuera del alcance al ser eliminada de la organización, seguirá suscrita a Shield Advanced. Dado que la cuenta ya no forma parte de la familia de facturación unificada, la cuenta generará una cuota de suscripción de Shield Advanced prorrateada. Por otro lado, una cuenta que queda fuera del alcance, pero permanece en la organización, no incurre en cargos adicionales.

Si un recurso queda fuera del alcance, seguirá protegido por Shield Advanced y seguirá incurriendo en gastos de transferencia de datos de Shield Advanced.

Mitigación automática de DDoS en la capa de aplicación

Cuando aplicas una política de Shield Advanced a CloudFront las distribuciones de Amazon o a los balanceadores de carga de aplicaciones, tienes la opción de configurar la mitigación automática de DDoS en la capa de aplicaciones de Shield Advanced en la política.

Para obtener información sobre la mitigación automática de Shield Advanced, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced.

La mitigación automática de DDoS en la capa de aplicación de Shield Advanced tiene los siguientes requisitos:

- La mitigación automática de DDoS en la capa de aplicaciones solo funciona con CloudFront las distribuciones de Amazon y los balanceadores de carga de aplicaciones.

Si aplicas tu política Shield Advanced a CloudFront las distribuciones de Amazon, puedes elegir esta opción para las políticas Shield Advanced que crees para la región global. Si aplica protecciones a los equilibradores de carga de aplicación, puede aplicar la política a cualquier región que admita Firewall Manager.

- La mitigación automática de DDoS a nivel de aplicación solo funciona con las ACL web que se crearon con la última versión de AWS WAF (v2).

  Por ello, si tiene una política que utiliza ACL web AWS WAF clásicas, tendrá que sustituir la política por una nueva, que utilizará automáticamente la última versión de AWS WAF, o bien hacer que Firewall Manager cree una nueva versión de las ACL web para su política actual y pase a utilizarlas. Para obtener más información sobre las opciones, consulte Sustituya las ACL web AWS WAF clásicas por las ACL web de última versión.

Configuración de mitigación automática

La opción de mitigación automática de DDoS en la capa de aplicación para las políticas de Firewall Manager Shield Advanced aplica la funcionalidad de mitigación automática de Shield Advanced a las cuentas y recursos incluidos en el alcance de su política. Para obtener información detallada sobre esta característica de Shield Advanced, consulte Mitigación de DDoS de la capa de aplicación automática de Shield Advanced.

Puede elegir que Firewall Manager habilite o deshabilite la mitigación automática para CloudFront las distribuciones o los balanceadores de carga de aplicaciones que estén dentro del ámbito de aplicación de la política, o puede elegir que la política ignore la configuración de mitigación automática de Shield Advanced:

- Activar: si decide activar la mitigación automática, también debe especificar si las reglas de mitigación de Shield Advanced deben contar o bloquear las solicitudes web coincidentes. Firewall Manager marcará los recursos dentro del alcance como no compatibles si no tienen activada la mitigación automática o si utilizan una acción de regla que no coincide con la que especificó para la política. Si configura la política para la corrección automática, Firewall Manager actualiza los recursos no compatibles según sea necesario.
- Desactivar: si decide desactivar la mitigación automática, Firewall Manager marcará los recursos dentro del alcance como no compatibles si tienen la mitigación automática activada. Si configura la política para la corrección automática, Firewall Manager actualiza los recursos no compatibles según sea necesario.

- Ignorar: si decide ignorar la mitigación automática, Firewall Manager no tendrá en cuenta ninguna de las configuraciones de mitigación automática de su política Shield cuando lleve a cabo actividades de corrección para la política. Esta configuración le permite controlar la mitigación automática a través de Shield Advanced, sin que Firewall Manager sobrescriba esa configuración. Esta configuración no se aplica a ningún recurso de equilibrador de carga clásico o IP elástica administrado a través de Shield Advanced, ya que Shield Advanced actualmente no admite la mitigación automática de nivel 7 para esos recursos.

Sustituya las ACL web AWS WAF clásicas por las ACL web de última versión

La mitigación automática de DDoS en la capa de aplicación solo funciona con las ACL web que se crearon con la última versión de AWS WAF (v2).

Para determinar la versión de ACL web de su política Shield Advanced, consulte Determinar la versión AWS WAF que utiliza una política de Shield Advanced.

Si desea utilizar la mitigación automática en su política de Shield Advanced y su política utiliza actualmente las ACL web AWS WAF clásicas, puede crear una nueva política de Shield Advanced para reemplazar la actual o puede utilizar las opciones descritas en esta sección para sustituir las ACL web de versiones anteriores por las ACL web nuevas (v2) incluidas en su política de Shield Advanced actual. Las nuevas políticas siempre crean ACL web con la última versión de. AWS WAF Si reemplaza la política completa, al eliminarla, puede hacer que Firewall Manager elimine también todas las ACL web de las versiones anteriores. En el resto de esta sección, se describen las opciones para reemplazar las ACL web incluidas en su política actual.

Al modificar una política Shield Advanced existente para CloudFront los recursos de Amazon, Firewall Manager puede crear automáticamente una nueva ACL web vacía AWS WAF (v2) para la política, en cualquier cuenta incluida en el ámbito que aún no tenga una ACL web v2. Cuando Firewall Manager crea una nueva ACL web, si la política ya tiene una ACL web AWS WAF clásica en la misma cuenta, Firewall Manager configura la nueva versión de la ACL web con la misma configuración de acción predeterminada que la ACL web existente. Si no existe una ACL web AWS WAF clásica, Firewall Manager establece la acción predeterminada Allow en la nueva ACL web. Después de que Firewall Manager cree una nueva ACL web, puede personalizarla según sea necesario a través de la consola AWS WAF .

Al elegir cualquiera de las siguientes opciones de configuración de políticas, Firewall Manager crea nuevas ACL web (v2) para las cuentas dentro del alcance que aún no las tienen:

- Al activar o desactivar la mitigación automática de DDoS en la capa de aplicación. Esta elección por sí sola solo hace que Firewall Manager cree las nuevas ACL web y no sustituya ninguna asociación de ACL web AWS WAF Classic existente en los recursos dentro del alcance de la política.
- Al elegir la acción política de corrección automática y elegir la opción de reemplazar las ACL web AWS WAF clásicas por las ACL web AWS WAF (v2). Puede optar por sustituir las ACL web de versiones anteriores independientemente de sus opciones de configuración para la mitigación automática de DDoS en la capa de aplicación.

  Al elegir la opción de reemplazo, Firewall Manager crea las ACL web de la nueva versión según sea necesario y luego hace lo siguiente para los recursos dentro del alcance de la política:
  - Si un recurso está asociado a una ACL web desde cualquier otra política activa del Firewall Manager, el Firewall Manager deja la asociación intacta.
  - En cualquier otro caso, Firewall Manager elimina cualquier asociación con una ACL web AWS WAF clásica y asocia el recurso con la ACL web AWS WAF (v2) de la política.

Puede elegir que Firewall Manager sustituya las ACL web de la versión anterior por las ACL web de la nueva versión cuando lo desee. Si ya ha personalizado las ACL web AWS WAF Classic de la política, puede actualizar las ACL web de la nueva versión a una configuración comparable antes de elegir que Firewall Manager realice el paso de sustitución.

Puede acceder a cualquier versión de la ACL web de una política a través de la consola de la misma versión AWS WAF o AWS WAF de la versión clásica.

Firewall Manager no elimina ninguna ACL web AWS WAF clásica sustituida hasta que elimine la propia política. Cuando la política deje de utilizar las ACL web AWS WAF clásicas, podrá eliminarlas si así lo desea.

Determinar la versión AWS WAF que utiliza una política de Shield Advanced

Para determinar qué versión de la AWS WAF política Firewall Manager Shield Advanced utiliza, consulte las claves de parámetros de la regla AWS Config vinculada a servicios de la política. Si la AWS WAF versión que se utiliza es la más reciente, las claves de parámetros incluyen `policyId` y. `webAclArn` Si se trata de la versión anterior, AWS WAF Classic, las claves de parámetro incluyen `webAclId` y`resourceTypes`.

La AWS Config regla solo enumera las claves de las ACL web que la política utiliza actualmente con los recursos incluidos en el ámbito de aplicación.

Para determinar qué versión de AWS WAF su política de Firewall Manager Shield Advanced utiliza

1. Recupere el identificador de política de la política Shield Advanced:

   a. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   b. En el panel de navegación, seleccione Políticas de Seguridad.

   c. Elija la región para la política. Para CloudFront las distribuciones, esto es`Global`.

   d. Busque la política que desea y copie el valor de su ID de política.

      ID de Política de ejemplo: `1111111-2222-3333-4444-a55aa5aaa555`.

2. Cree el nombre de la AWS Config regla de la política añadiendo el ID de la política a la cadena. `FMManagedShieldConfigRule`

   Ejemplo de nombre de AWS Config regla:`FMManagedShieldConfigRule1111111-2222-3333-4444-a55aa5aaa555`.

3. Busque en los parámetros de la AWS Config regla asociada las claves denominadas `policyId` y`webAclArn`:

   a. Abra la AWS Config consola en https://console.aws.amazon.com/config/.

   b. En el panel de navegación, seleccione Reglas.

   c. Busque el nombre de la AWS Config regla de la política de Firewall Manager en la lista y selecciónelo. Se abre la página de la regla.

   d. En la sección Parámetros de Detalles de las reglas, observe las claves. Si encuentra claves denominadas `policyId` y `webAclArn`, la política utiliza las ACL web que se crearon con la versión más reciente de AWS WAF. Si encuentra claves denominadas `webAclId` y`resourceTypes`, la política utiliza las ACL web que se crearon con la versión anterior, la AWS WAF clásica.

Políticas de grupos de seguridad

Puede usar políticas AWS Firewall Manager de grupos de seguridad para administrar los grupos de seguridad de Amazon Virtual Private Cloud para su organización en AWS Organizations. Puede

aplicar políticas de grupos de seguridad controladas centralmente a toda la organización o a un subconjunto seleccionado de cuentas y recursos. También puede supervisar y administrar las políticas de grupos de seguridad que están en uso en su organización, con políticas de grupos de seguridad de auditoría y uso.

Firewall Manager mantiene continuamente sus políticas y las aplica a cuentas y recursos a medida que se agregan o actualizan en toda la organización. Para obtener más información al respecto AWS Organizations, consulte la Guía AWS Organizations del usuario.

Para obtener información sobre los grupos de seguridad de Amazon Virtual Private Cloud, consulte Grupos de seguridad para su VPC en la Guía del usuario de Amazon VPC.

Puede utilizar política de grupo de seguridad de Firewall Manager para realizar lo siguiente en toda la organización de AWS :

- Aplicar grupos de seguridad comunes a cuentas y recursos especificados.
- Auditar reglas de grupo de seguridad para localizar y corregir reglas no conformes.
- Auditar el uso de grupos de seguridad para eliminar grupos de seguridad no utilizados y redundantes.

En esta sección se describe cómo funcionan las política de grupos de seguridad de Firewall Manager y se proporciona orientación para utilizarlas. Para obtener información sobre los procedimientos para crear políticas de grupos de seguridad, consulte Creación de una AWS Firewall Manager política.

Políticas de grupos de seguridad comunes

Con una política de grupo de seguridad común, Firewall Manager proporciona una asociación controlada centralmente de grupos de seguridad con cuentas y recursos de toda la organización. Especifique dónde y cómo aplicar la política en su organización.

Puede aplicar políticas de grupos de seguridad comunes a los siguientes tipos de recursos:

- Instancia de Amazon Elastic Compute Cloud (Amazon EC2)
- Elastic Network Interface
- Equilibrador de carga de aplicación
- Equilibrador de carga clásico

Para obtener instrucciones sobre cómo crear una política de grupo de seguridad común mediante la consola, consulte Crear una política de grupo de seguridad común.

VPC compartidas

En la configuración de ámbito de política de una política de grupo de seguridad común, puede optar por incluir VPC compartidas. Esta opción incluye VPC que son propiedad de otra cuenta y que se comparten con una cuenta dentro del ámbito. Las VPC que poseen cuentas dentro del ámbito siempre se incluyen. Para obtener información sobre las VPC compartidas, consulte Trabajar con VPC compartidas en la Guía del usuario de Amazon VPC.

Las siguientes advertencias se aplican a la hora de incluir VPC compartidas. Estas advertencias se suman a las advertencias generales sobre las políticas de grupos de seguridad que se encuentran en Advertencias y limitaciones de las políticas de los grupos de seguridad.

- Firewall Manager replica el grupo de seguridad principal en las VPC para cada cuenta dentro del ámbito. Para una VPC compartida, Firewall Manager replica el grupo de seguridad principal una vez para cada cuenta dentro del ámbito con la que se comparte la VPC. Esto puede dar lugar a varias réplicas en una única VPC compartida.
- Al crear una VPC compartida nueva, no la verá representada en los detalles de la política de grupo de seguridad de Firewall Manager hasta después de crear al menos un recurso en la VPC que esté dentro del ámbito de la política.
- Cuando deshabilita las VPC compartidas en una política que tenía las VPC compartidas habilitadas, en las VPC compartidas, Firewall Manager elimina los grupos de seguridad de réplica que no están asociados a ningún recurso. Firewall Manager deja los grupos de seguridad de réplica restantes en su lugar, pero deja de administrarlos. La eliminación de estos grupos de seguridad restantes requiere la administración manual en cada instancia de VPC compartida.

Grupos de seguridad principales

Para cada política de grupo de seguridad común, se AWS Firewall Manager proporcionan uno o más grupos de seguridad principales:

- Los grupos de seguridad principales deben ser creados por la cuenta de administrador de Firewall Manager y pueden residir en cualquier instancia de Amazon VPC de la cuenta.
- Puede administrar grupos de seguridad principal a través de Amazon Virtual Private Cloud (Amazon VPC) o Amazon Elastic Compute Cloud (Amazon EC2). Para obtener información, consulte Uso de grupos de seguridad en la Guía del usuario de Amazon VPC.

- Puede nombrar uno o varios grupos de seguridad como principales para una política de grupo de seguridad de Firewall Manager. De forma predeterminada, el número de grupos de seguridad permitidos en una política es uno, pero puede enviar una solicitud para aumentarlo. Para obtener más información, consulte AWS Firewall Manager cuotas.

Configuración de reglas de la política

Puede elegir uno o más de los siguientes comportamientos de control de cambios para los grupos de seguridad y los recursos de la política de grupo de seguridad común:

- Identifique y reporte los cambios realizados por los usuarios locales en los grupos de seguridad de réplica.
- Desasocie cualquier otro grupo de seguridad de los AWS recursos que estén dentro del ámbito de la política.
- Distribuya las etiquetas del grupo primario a los grupos de seguridad de réplica.

> **Important**
>
> Firewall Manager no distribuirá las etiquetas de sistema agregadas por AWS los servicios en los grupos de seguridad de réplica. Las etiquetas del sistema comienzan por el prefijo `aws:`. Además, Firewall Manager no actualizará las etiquetas de los grupos de seguridad existentes ni creará nuevos grupos de seguridad si la política tiene etiquetas que entren en conflicto con la política de etiquetas de la organización. Para obtener información sobre las políticas de etiquetas, consulte las políticas de etiquetas en la Guía del AWS Organizations usuario.

- Distribuya las referencias del grupo de seguridad de los grupos principales a los grupos de seguridad de réplica.

  Esto le permite establecer fácilmente reglas de referencia de grupos de seguridad comunes en todos los recursos incluidos en el alcance para las instancias asociadas a la VPC del grupo de seguridad especificado. Al activar esta opción, Firewall Manager solo propaga las referencias a los grupos de seguridad si los grupos de seguridad hacen referencia a grupos de seguridad homólogos en Amazon Virtual Private Cloud. Si los grupos de seguridad de réplica no hacen referencia correctamente al grupo de seguridad homólogo, Firewall Manager marca estos grupos de seguridad replicados como no conformes. Para obtener información sobre cómo hacer referencia a los grupos de seguridad homólogos en Amazon VPC, consulte Actualizar los

grupos de seguridad para hacer referencia a los grupos de seguridad homólogos en la Guía de emparejamiento de Amazon VPC.

Si no habilita esta opción, Firewall Manager no propaga las referencias a los grupos de seguridad de réplica. Para obtener información sobre la interconexión de VPC en Amazon VPC, consulte la Guía de interconexión de Amazon VPC.

Creación y gestión de políticas

Al crear la política de grupo de seguridad común, Firewall Manager replica los grupos de seguridad principales en cada instancia de Amazon VPC dentro del ámbito de la política y asocia los grupos de seguridad replicados a cuentas y recursos incluidos en el ámbito de la política. Al modificar un grupo de seguridad principal, Firewall Manager propaga el cambio a las réplicas.

Al eliminar una política de grupo de seguridad común, puede elegir si desea borrar los recursos creados por la política. Para los grupos de seguridad comunes de Firewall Manager, estos recursos son los grupos de seguridad de réplica. Elija la opción de eliminación a menos que desee administrar manualmente cada réplica individual después de eliminar la política. En la mayoría de las situaciones, elegir la opción de eliminación es el enfoque más sencillo.

Cómo se administran las réplicas

Los grupos de seguridad de réplica de las instancias de Amazon VPC se administran como otros grupos de seguridad de Amazon VPC. Para obtener información, consulte Grupos de seguridad de su VPC en la Guía del usuario de Amazon VPC.

Políticas de grupos de seguridad de auditoría de contenido

Utilice las políticas de los grupos de seguridad de auditoría de AWS Firewall Manager contenido para auditar y aplicar acciones políticas a las reglas que se utilizan en los grupos de seguridad de su organización. Las políticas de grupos de seguridad de auditoría de contenido se aplican a todos los grupos de seguridad creados por los clientes que se utilizan en su AWS organización, según el ámbito que defina en la política.

Para obtener instrucciones sobre cómo crear una política de grupo de seguridad de auditoría de contenido mediante la consola, consulte Crear una política de grupo de seguridad de auditoría de contenido.

Tipo de recurso de ámbito de la política

Puede aplicar políticas de grupos de seguridad de auditoría de contenido a los siguientes tipos de recursos:

- Instancia de Amazon Elastic Compute Cloud (Amazon EC2)
- Elastic Network Interface
- Grupo de seguridad de Amazon VPC

Los grupos de seguridad se consideran dentro del ámbito de la política si están explícitamente dentro del ámbito o si están asociados con recursos que están dentro del ámbito.

Opciones de la regla de política

Puede usar reglas de política administradas o reglas de política personalizadas para cada política de auditoría de contenido, pero no ambas.

- Reglas de políticas administradas: en una política con reglas administradas, puede usar listas de aplicaciones y de protocolos para controlar las reglas que Firewall Manager audita y marca como compatibles o no compatibles. Puede usar listas administradas por el Firewall Manager. También puede crear y usar sus propias listas de aplicaciones y de protocolos. Para obtener información sobre estos tipos de listas y sus opciones de administración para las listas personalizadas, consulte Listas administradas.
- Reglas de política personalizadas: en una política con reglas de política personalizadas, especifique un grupo de seguridad existente como grupo de seguridad de auditoría para su política. Puede usar las reglas del grupo de seguridad de auditoría como plantilla que defina las reglas que Firewall Manager audita y marca como compatibles o no compatibles.

Auditar grupos de seguridad

Debe crear grupos de seguridad de auditoría con su cuenta de administrador de Firewall Manager para poder usarlos en su política. Puede administrar grupos de seguridad a través de Amazon Virtual Private Cloud (Amazon VPC) o Amazon Elastic Compute Cloud (Amazon EC2). Para obtener información, consulte Uso de grupos de seguridad en la Guía del usuario de Amazon VPC.

Firewall Manager solo utiliza un grupo de seguridad que utiliza para una política de grupo de seguridad de auditoría de contenido como referencia de comparación para los grupos de seguridad incluidos en el ámbito de la política. Firewall Manager no lo asocia con ningún recurso de su organización.

La forma en que defina las reglas en el grupo de seguridad de auditoría depende de sus elecciones en la configuración de reglas de la política:

- Reglas de políticas administradas: para la configuración de las reglas de políticas administradas, se utiliza un grupo de seguridad de auditoría para anular otras configuraciones de la política y permitir o denegar explícitamente las reglas que, de otro modo, podrían tener otro resultado de compatibilidad.
  - Si decide permitir siempre las reglas definidas en el grupo de seguridad de auditoría, cualquier regla que coincida con una que esté definida en el grupo de seguridad de auditoría se considerará compatible con la política, independientemente de las demás configuraciones de la política.
  - Si decide denegar siempre las reglas definidas en el grupo de seguridad de auditoría, cualquier regla que coincida con una que esté definida en el grupo de seguridad de auditoría se considerará incompatible con la política, independientemente de las demás configuraciones de la política.
- Reglas de políticas personalizadas: en el caso de la configuración de reglas de políticas personalizadas, el grupo de seguridad de auditoría proporciona un ejemplo de lo que es aceptable o no aceptable en las reglas del grupo de seguridad incluidas en el alcance:
  - Si decide permitir el uso de las reglas, todos los grupos de seguridad dentro del alcance solo deben tener reglas que estén dentro del rango permitido de las reglas de grupo de seguridad de auditoría de la política. En este caso, las reglas de grupo de seguridad de la política proporcionan el ejemplo de lo que es aceptable hacer.
  - Si decide denegar el uso de las reglas, todos los grupos de seguridad dentro del alcance solo deben tener reglas que no estén dentro del rango permitido de las reglas de grupo de seguridad de auditoría de la política. En este caso, el grupo de seguridad de la política proporciona el ejemplo de lo que no es aceptable hacer.

Creación y gestión de políticas

Al crear una política de grupo de seguridad de auditoría, debe tener deshabilitada la corrección automática. Se recomienda revisar los efectos de la creación de políticas antes de habilitar la corrección automática. Después de revisar los efectos esperados, puede editar la política y habilitar la corrección automática. Cuando la corrección automática está habilitada, Firewall Manager actualiza o quita reglas que no son conformes de los grupos de seguridad dentro del ámbito.

Grupos de seguridad afectados por una política de grupo de seguridad de auditoría

Todos los grupos de seguridad de la organización creados por el cliente pueden incluirse en el ámbito de una política de grupo de seguridad de auditoría.

Los grupos de seguridad de réplica no son creados por el cliente y, por lo tanto, no son aptos para incluirse directamente en el ámbito de una política de grupo de seguridad de auditoría. Sin embargo, se pueden actualizar como resultado de las actividades de corrección automática de la política. El grupo de seguridad principal de una política de grupo de seguridad común es creado por el cliente y puede incluirse en el ámbito de una política de grupo de seguridad de auditoría. Si una política de grupo de seguridad de auditoría realiza cambios en un grupo de seguridad principal, Firewall Manager propaga automáticamente esos cambios a las réplicas.

Políticas de grupos de seguridad de auditoría de uso

Utilice las políticas AWS Firewall Manager de auditoría de uso de los grupos de seguridad para supervisar su organización en busca de grupos de seguridad redundantes o no utilizados y, si lo desea, realice una limpieza. Al habilitar la corrección automática para esta política, Firewall Manager hace lo siguiente:

1. Consolida grupos de seguridad redundantes, si ha elegido esa opción.
2. Elimina los grupos de seguridad no utilizados, si ha elegido esa opción.

Puede aplicar políticas de grupos de seguridad de auditoría de uso a los siguientes tipos de recursos:

- Grupo de seguridad de Amazon VPC

Para obtener instrucciones sobre cómo crear una política de grupo de seguridad de auditoría de uso mediante la consola, consulte Crear una política de grupo de seguridad de auditoría de uso.

Cómo detecta y corrige Firewall Manager los grupos de seguridad redundantes

Para que los grupos de seguridad se consideren redundantes, deben tener exactamente las mismas reglas establecidas y estar en la misma instancia de Amazon VPC.

Para corregir un conjunto de grupos de seguridad redundante, Firewall Manager selecciona uno de los grupos de seguridad del conjunto que desea conservar y, a continuación, lo asocia a todos los recursos que están asociados a los demás grupos de seguridad del conjunto. A continuación, Firewall Manager desasocia los demás grupos de seguridad de los recursos a los que estaban asociados, lo que hace que no se utilicen.

> **Note**
>
> Si también ha elegido eliminar los grupos de seguridad no utilizados, Firewall Manager los elimina a continuación. Esto puede dar lugar a la eliminación de los grupos de seguridad que están en el conjunto redundante.

Cómo detecta y corrige Firewall Manager los grupos de seguridad no utilizados

Firewall Manager considera que un grupo de seguridad no se utiliza si se cumplen las dos condiciones siguientes:

- Ninguna instancia de Amazon EC2 ni la interfaz de red elástica de Amazon EC2 utilizan el grupo de seguridad.
- Firewall Manager no ha recibido ningún elemento de configuración correspondiente en el número de minutos especificado en el período de tiempo de la regla de política.

El período de tiempo de la regla de política tiene una configuración predeterminada de cero minutos, pero puede aumentarlo hasta 365 días (525 600 minutos) para tener tiempo de asociar nuevos grupos de seguridad a los recursos.

> **Important**
>
> Si especifica un número de minutos distinto del valor predeterminado de cero, debe habilitar las relaciones indirectas. AWS Config De lo contrario, las políticas de los grupos de seguridad de auditoría de uso no funcionarán según lo previsto. Para obtener información sobre las relaciones indirectas en AWS Config, consulte Relaciones indirectas AWS Config en la Guía para AWS Config desarrolladores.

Firewall Manager corrige los grupos de seguridad no utilizados eliminándolos de su cuenta de acuerdo con la configuración de sus reglas, si es posible. Si Firewall Manager no puede eliminar un grupo de seguridad, lo marca como no compatible con la política. Firewall Manager no puede eliminar un grupo de seguridad al que hace referencia otro grupo de seguridad.

La duración de la corrección varía en función de si se utiliza la configuración de período de tiempo predeterminada o una configuración personalizada:

- Período de tiempo establecido en cero, el valor predeterminado: con esta configuración, un grupo de seguridad se considera no utilizado cuando una instancia de Amazon EC2 o una interfaz de red elástica no lo utilizan.

  Para esta configuración de período de tiempo cero, Firewall Manager corrige el grupo de seguridad inmediatamente.
- Período de tiempo superior a cero: con esta configuración, un grupo de seguridad se considera no utilizado cuando no lo está utilizando una instancia Amazon EC2 o una interfaz de red elástica y Firewall Manager no ha recibido un elemento de configuración para él en el plazo de minutos especificado.

  Para la configuración de período de tiempo distinto de cero, Firewall Manager corrige el grupo de seguridad después de que haya permanecido en estado no utilizado durante 24 horas.

Especificación de cuenta predeterminada

Al crear una política de grupo de seguridad de auditoría de uso a través de la consola, Firewall Manager selecciona automáticamente Excluir las cuentas especificadas e incluir todas las demás. A continuación, el servicio pone la cuenta de administrador de Firewall Manager en la lista de exclusión. Esta es la estrategia recomendada y le permite administrar manualmente los grupos de seguridad que pertenecen a la cuenta de administrador de Firewall Manager.

Prácticas recomendadas para las políticas de grupos de seguridad

En esta sección aparecen recomendaciones para administrar grupos de seguridad mediante AWS Firewall Manager.

Excluir la cuenta de administrador de Firewall Manager

Cuando establezca el ámbito de la política, excluya la cuenta de administrador de Firewall Manager. Cuando crea una política de grupo de seguridad de auditoría de uso a través de la consola, esta es la opción predeterminada.

Comience con la corrección automática desactivada

Para políticas de grupos de seguridad de auditoría de contenido o uso, comience con la corrección automática deshabilitada. Revise la información de detalles de la política para determinar los efectos que tendría la corrección automática. Cuando esté convencido de que los cambios son lo que desea, edite la política y habilite la corrección automática.

Evite conflictos si también utiliza fuentes externas para administrar grupos de seguridad

Si utiliza una herramienta o servicio que no sea Firewall Manager para administrar los grupos de seguridad, tenga cuidado de evitar conflictos entre su configuración en Firewall Manager y la configuración en su fuente externa. Si utiliza la corrección automática y su configuración entra en conflicto, puede crear un ciclo de corrección conflictiva que consuma recursos en ambos lados.

Por ejemplo, supongamos que configura que otro servicio mantenga un grupo de seguridad para un conjunto de recursos de AWS y configura una política de Firewall Manager para que mantenga un grupo de seguridad diferente para algunos o todos los mismos recursos. Si configura que cualquier parte no permita que cualquier otro grupo de seguridad se asocie con los recursos dentro del ámbito, esa parte eliminará la asociación del grupo de seguridad que mantiene la otra marte. Si ambas partes se configuran de esta manera, puede acabar con un ciclo de asociaciones y desasociaciones conflictivas.

Además, supongamos que crea una política de auditoría de Firewall Manager para aplicar una configuración de grupo de seguridad que entra en conflicto con la configuración de grupo de seguridad del otro servicio. La corrección aplicada por la política de auditoría de Firewall Manager puede actualizar o eliminar ese grupo de seguridad, lo que hace que esté fuera de la conformidad del otro servicio. Si el otro servicio está configurado para supervisar y solucionar automáticamente cualquier problema que encuentre, volverá a crear o actualizar el grupo de seguridad, haciendo de nuevo que esté fuera de la conformidad con la política de auditoría de Firewall Manager. Si la política de auditoría de Firewall Manager está configurada con corrección automática, volverá a actualizar o eliminar el grupo de seguridad externo, etc.

Para evitar conflictos como estos, cree configuraciones que sean mutuamente excluyentes, entre Firewall Manager y cualquier fuente externa.

Puede utilizar el etiquetado para excluir grupos de seguridad externos de la corrección automática por parte de las políticas de Firewall Manager. Para ello, agregue una o más etiquetas a los grupos de seguridad u otros recursos administrados por la fuente externa. A continuación, cuando defina el ámbito de la política de Firewall Manager, en la especificación de recursos, excluya los recursos que tengan la etiqueta o las etiquetas que haya agregado.

Del mismo modo, en su herramienta o servicio externo, excluya los grupos de seguridad que Firewall Manager administra de cualquier actividad de administración o auditoría. O bien no importe los recursos de Firewall Manager o use etiquetas específicas de Firewall Manager para excluirlos de la administración externa.

Prácticas recomendadas para la auditoría de uso de las políticas de los grupos de seguridad

Siga estas pautas cuando utilice políticas de grupos de seguridad de auditoría de uso.

- Evite realizar varios cambios en el estado de asociación de un grupo de seguridad en un período corto de tiempo, por ejemplo, en un período de 15 minutos. Si lo hace, es posible que Firewall Manager se pierda algunos o todos los eventos correspondientes. Por ejemplo, no asocie y desasocie rápidamente un grupo de seguridad con una interface de red elástica.

Advertencias y limitaciones de las políticas de los grupos de seguridad

En esta sección se enumeran las advertencias y limitaciones relacionadas con el uso de las políticas de grupos de seguridad de Firewall Manager:

- No se admite la actualización de grupos de seguridad para interfaces de red elásticas de Amazon EC2 creadas con el tipo de servicio Fargate. Sin embargo, puede actualizar grupos de seguridad para interfaces de red elásticas de Amazon ECS con el tipo de servicio de Amazon EC2.
- Firewall Manager no admite grupos de seguridad para las interfaces de red elásticas de Amazon EC2 que creadas por Amazon Relational Database Service (Servicio de base de datos relacional de Amazon).
- La actualización de interfaces de red elásticas de Amazon ECS solo es posible para los servicios de Amazon ECS que utilizan el controlador de implementación de actualización continua (Amazon ECS). Para otros controladores de implementación de Amazon ECS, como CODE_DEPLOY o controladores externos, en estos momentos, Firewall Manager no puede actualizar las interfaces de red elásticas.
- Con los grupos de seguridad para las interfaces de red elásticas de Amazon EC2, los cambios en un grupo de seguridad no son visibles inmediatamente para Firewall Manager. Firewall Manager suele detectar los cambios al cabo de varias horas, pero la detección puede demorarse hasta seis horas.
- Firewall Manager no admite la actualización de grupos de seguridad en interfaces de red elásticas para equilibradores de carga de red.
- En las políticas de grupos de seguridad comunes, si una VPC compartida luego deja de compartirse con una cuenta, Firewall Manager no eliminará los grupos de seguridad de réplica de la cuenta.
- Con las políticas de grupos de seguridad de auditoría de uso, si crea varias políticas con una configuración de tiempo de demora personalizada y todas con el mismo alcance, la primera política en la que se determine el cumplimiento será la política que informe de los hallazgos.

Casos de uso de políticas de grupos de seguridad

Puede usar políticas de grupos de seguridad AWS Firewall Manager comunes para automatizar la configuración del firewall del host para la comunicación entre las instancias de Amazon VPC. En esta sección se enumeran las arquitecturas estándar de Amazon VPC y se describe cómo proteger cada una mediante políticas de grupos de seguridad comunes de Firewall Manager. Estas políticas de grupos de seguridad pueden ayudarle a aplicar un conjunto unificado de reglas para seleccionar recursos en diferentes cuentas y evitar configuraciones por cuenta en Amazon Elastic Compute Cloud y Amazon VPC.

Con las políticas de grupos de seguridad comunes de Firewall Manager, puede etiquetar solo las interfaces de red elásticas de EC2 que necesita para comunicarse con instancias de otra Amazon VPC. Las otras instancias en la misma Amazon VPC quedan entonces más seguras y aisladas.

Caso de uso: supervisión y control de las solicitudes a los equilibradores de carga de aplicación y a los equilibradores de carga clásicos

Puede usar una política de grupo de seguridad común de Firewall Manager para definir qué solicitudes deben atender sus equilibradores de carga internos. Puede configurar esto a través de la consola del Firewall Manager. Solo las solicitudes que cumplan con las reglas de entrada del grupo de seguridad pueden llegar a sus equilibradores de carga, y los equilibradores de carga solo distribuirán las solicitudes que cumplan con las reglas de salida.

Caso de uso: VPC de Amazon pública y accesible a través de Internet

Puede utilizar una política de grupo de seguridad común de Firewall Manager para proteger una VPC de Amazon pública, por ejemplo, para permitir solo el puerto de entrada 443. Esto es lo mismo que permitir el tráfico HTTPS entrante para una VPC pública. Puede etiquetar recursos públicos dentro de la VPC (por ejemplo, como “PublicVPC”) y, a continuación, establecer el alcance de la política de Firewall Manager solo a los recursos con esa etiqueta. Firewall Manager aplica automáticamente la política a esos recursos.

Caso de uso: instancias públicas y privadas de Amazon VPC

Puede utilizar la misma política de grupo de seguridad común para recursos públicos que se recomienda en el caso de uso anterior para instancias de Amazon VPC públicas accesibles por Internet. Puede utilizar una segunda política de grupo de seguridad común para limitar la comunicación entre los recursos públicos y los privados. Etiquete los recursos de las instancias públicas y privadas de Amazon VPC con algo como "PublicPrivate" para aplicarles la segunda

política. Puede utilizar una tercera política para definir la comunicación permitida entre los recursos privados y otras instancias de Amazon VPC corporativas o privadas. Para esta política, puede utilizar otra etiqueta de identificación en los recursos privados.

Caso de uso: instancias de Amazon VPC de concentradores y radios

Puede utilizar una política de grupo de seguridad común para definir las comunicaciones entre la instancia de Amazon VPC de concentrador y las instancias de Amazon VPC de radio. Puede utilizar una segunda política para definir la comunicación desde cada instancia de Amazon VPC de radio a la instancia de Amazon VPC de concentrador.

Caso de uso: interfaz de red predeterminada para instancias Amazon EC2

Puede utilizar una política de grupo de seguridad común para permitir únicamente comunicaciones estándar, por ejemplo, servicios de actualización de parche/SO y SSH internos y para no permitir otras comunicaciones inseguras.

Caso de uso: identificar recursos con permisos abiertos

Puede utilizar una política de grupo de seguridad de auditoría para identificar todos los recursos de la organización que tienen permiso para comunicarse con direcciones IP públicas o que tienen direcciones IP que pertenecen a proveedores externos.

Políticas de listas de control de acceso (ACL) a la red de Amazon VPC

En esta sección se explica cómo funcionan las políticas de ACL de AWS Firewall Manager red y se proporcionan instrucciones para utilizarlas. Para obtener instrucciones sobre cómo crear una política de ACL de red mediante la consola, consulteCrear una política de ACL de red.

Para obtener información sobre las listas de control de acceso a la red (ACL) de Amazon VPC, consulte Control del tráfico a las subredes mediante ACL de red en la Guía del usuario de Amazon VPC.

Puede utilizar las políticas de ACL de red de Firewall Manager para gestionar las listas de control de acceso (ACL) a la red de Amazon Virtual Private Cloud (Amazon VPC) para su organización. AWS Organizations Usted define la configuración de las reglas de ACL de red de la política y las cuentas y subredes en las que desea que se aplique la configuración. Firewall Manager aplica continuamente la configuración de sus políticas a las cuentas y subredes a medida que se agregan o actualizan en toda la organización. Para obtener información sobre el alcance de la política AWS Organizations, consulte AWS Firewall Manager alcance de la política la Guía del AWS Organizations usuario.

Al definir una política de ACL de red de Firewall Manager, además de la configuración estándar de la política de Firewall Manager, como el nombre y el alcance, debe proporcionar lo siguiente:

- Primera y última regla para la gestión del tráfico entrante y saliente. Firewall Manager impone la presencia y el orden de estos elementos en las ACL de la red que están dentro del ámbito de aplicación de la política o informa de su incumplimiento. Sus cuentas individuales pueden crear reglas personalizadas que se ejecuten entre la primera y la última regla de la política.
- Si se debe forzar la corrección cuando la remediación pueda provocar conflictos en la administración del tráfico entre las reglas de la ACL de la red. Esto se aplica solo cuando la corrección está habilitada para la política.

Reglas y etiquetado de ACL de red de Firewall Manager

En esta sección se describen las especificaciones de las reglas de política de ACL de red y las ACL de red que administra Firewall Manager.

Etiquetado en una ACL de red gestionada

Firewall Manager etiqueta una ACL de red administrada con una `FMManaged` etiqueta que tiene un valor de`true`. Firewall Manager solo corrige las ACL de red que tienen esta configuración de etiqueta.

Reglas que usted defina en la política

En la especificación de la política de ACL de la red, usted define las reglas que desea ejecutar primero y último para el tráfico entrante y las reglas que desea ejecutar primero y último para el tráfico saliente.

De forma predeterminada, puede definir hasta 5 reglas de entrada para usarlas en cualquier combinación de la primera y la última regla de la política. Del mismo modo, puede definir hasta 5 reglas de salida. Para obtener más información sobre estos límites, consulteCuotas flexibles. Para obtener información sobre los límites generales de las ACL de red, consulte las cuotas de Amazon VPC en las ACL de red en la Guía del usuario de Amazon VPC.

No se asignan números de regla a las reglas de la política. En su lugar, usted especifica las reglas en el orden en que desea que se evalúen y Firewall Manager utiliza ese orden para asignar números de reglas en las ACL de red que administra.

Además, administra las especificaciones de las reglas de ACL de red de la política del mismo modo que administraría las reglas de una ACL de red a través de Amazon VPC. Para obtener información

sobre la administración de ACL de red en Amazon VPC, consulte Controlar el tráfico a las subredes mediante ACL de red y Trabajar con ACL de red en la Guía del usuario de Amazon VPC.

Reglas en una red gestionada (ACL)

Firewall Manager configura las reglas en una ACL de red que administra colocando la primera y la última regla de la política antes y después de cualquier regla personalizada que defina un administrador de cuentas individual. Firewall Manager conserva el orden de las reglas personalizadas. Las ACL de red se evalúan a partir de la regla con el número más bajo.

Cuando Firewall Manager crea por primera vez una ACL de red, define las reglas con la siguiente numeración:

- Primeras reglas: 1, 2,... — Definido por usted en la política de ACL de la red del Firewall Manager.

  Firewall Manager asigna números de regla a partir de 1 con incrementos de 1, con las reglas ordenadas tal como las ha ordenado en la especificación de la política.
- Reglas personalizadas: 5.000, 5.100,... — Administrado por administradores de cuentas individuales a través de Amazon VPC.

  Firewall Manager asigna números a estas reglas empezando por 5.000 y aumentando en 100 para cada regla subsiguiente.
- Últimas reglas:... 32.765, 32.766: Definido por usted en la política de ACL de red del Firewall Manager.

  Firewall Manager asigna números de regla que terminan en el número más alto posible, 32766 con incrementos de 1, con las reglas ordenadas tal como las ha ordenado en la especificación de la política.

Tras la inicialización de las ACL de red, Firewall Manager no controla los cambios que las cuentas individuales realizan en sus ACL de red gestionadas. Las cuentas individuales pueden cambiar una ACL de red sin infringir la normativa, siempre que las reglas personalizadas permanezcan numeradas entre la primera y la última regla de la política, y que la primera y la última regla mantengan el orden especificado. Como práctica recomendada, cuando gestione reglas personalizadas, siga la numeración que se describe en esta sección.

Cómo inicia Firewall Manager la administración de ACL de red para una subred

Firewall Manager comienza a administrar la ACL de red de una subred cuando asocia la subred a una ACL de red que Firewall Manager ha creado y marcado como `FMManaged` establecida. `true`

El cumplimiento de una política de ACL de red requiere que la ACL de red de la subred coloque las primeras reglas de la política en primer lugar, en el orden especificado en la política, las últimas en último lugar, en orden, y cualquier otra regla personalizada en el medio. Estos requisitos se pueden cumplir con una ACL de red no administrada a la que la subred ya esté asociada o con una ACL de red administrada.

Cuando Firewall Manager aplica una política de ACL de red a una subred asociada a una ACL de red no administrada, Firewall Manager comprueba lo siguiente en orden y se detiene cuando identifica una opción viable:

1. La ACL de red asociada ya es compatible: si la ACL de red que está actualmente asociada a la subred es compatible, Firewall Manager deja esa asociación en su lugar y no inicia la administración de la ACL de red para la subred.

   Firewall Manager no altera ni administra de otro modo una ACL de red que no sea de su propiedad, pero siempre que sea compatible, Firewall Manager la deja en su lugar y se limita a supervisarla para comprobar el cumplimiento de las políticas.
2. Hay disponible una ACL de red administrada compatible: si Firewall Manager ya administra una ACL de red que cumple con la configuración requerida, esta es una opción. Si la corrección está habilitada, el Firewall Manager le asocia la subred. Si la corrección está deshabilitada, Firewall Manager marca la subred como no compatible y ofrece reemplazar la asociación de ACL de la red como opción de corrección.
3. Cree una nueva ACL de red gestionada compatible: si la corrección está habilitada, Firewall Manager crea una nueva ACL de red y la asocia a la subred. De lo contrario, Firewall Manager marca la subred como no compatible y ofrece las opciones correctivas de crear la nueva ACL de red y reemplazar la asociación de ACL de red.

Si estos pasos no se realizan correctamente, Firewall Manager informa del incumplimiento de la subred.

Firewall Manager sigue estos pasos cuando una subred entra en el alcance por primera vez y cuando la ACL de la red no administrada de una subred no cumple con las normas.

Cómo corrige Firewall Manager las ACL de red gestionadas que no cumplen las normas

En esta sección se describe cómo Firewall Manager corrige sus ACL de red gestionadas cuando no cumplen con la política. Firewall Manager solo corrige las ACL de red administradas, con la etiqueta configurada en`FMManaged`. `true` Para ver las ACL de red que no están administradas por Firewall Manager, consulte[Administración inicial de las ACL de red](#).

La corrección restaura las ubicaciones relativas de la primera regla, la personalizada y la última, y restablece el orden de la primera y la última regla. Durante la corrección, Firewall Manager no necesariamente moverá las reglas a los números de regla que utiliza en la inicialización de la ACL de la red. Para ver la configuración numérica inicial y las descripciones de estas categorías de reglas, consulte. [Administración inicial de las ACL de red](#)

Para establecer reglas y un orden de reglas compatibles, es posible que Firewall Manager necesite mover las reglas dentro de la ACL de la red. En la medida de lo posible, Firewall Manager preserva las protecciones de la ACL de la red manteniendo al mismo tiempo el orden de normas vigente. Por ejemplo, podría duplicar temporalmente las reglas en nuevas ubicaciones y, a continuación, eliminar ordenadamente las reglas originales, conservando las ubicaciones relativas durante el proceso.

Este enfoque protege la configuración, pero también requiere espacio en la ACL de la red para las reglas provisionales. Si Firewall Manager alcanza el límite de reglas en una ACL de red, detendrá la corrección. Cuando esto ocurre, la ACL de la red sigue sin cumplir las normas y Firewall Manager informa del motivo.

Si una cuenta agrega reglas personalizadas a una ACL de red administrada por Firewall Manager y esas reglas interfieren con la corrección del Firewall Manager, Firewall Manager detiene cualquier actividad de corrección en la ACL de red e informa del conflicto.

Solución forzosa

Si elige la corrección automática para la política, también especifica si desea forzar la corrección para la primera regla o para la última regla.

Cuando Firewall Manager detecta un conflicto en la gestión del tráfico entre una regla personalizada y una regla de política, hace referencia a la configuración de corrección forzada correspondiente. Si la corrección forzada está habilitada, Firewall Manager la aplica a pesar del conflicto. Si esta opción no está habilitada, el Firewall Manager detiene la corrección. En cualquier caso, Firewall Manager informa del conflicto de reglas y ofrece opciones de corrección.

Requisitos y limitaciones del recuento de reglas

Durante la corrección, Firewall Manager puede duplicar temporalmente las reglas para moverlas sin alterar las protecciones que proporcionan.

Tanto para las reglas de entrada como de salida, el mayor número de reglas que Firewall Manager puede necesitar para corregir es el siguiente:

```
2 * (the number of rules defined in the policy for the traffic direction)
+
the number of custom rules defined in the network ACL for the traffic direction
```

Las ACL de red y las políticas de ACL de red están sujetas a límites de reglas mutables. Si Firewall Manager alcanza un límite en sus esfuerzos de remediación, deja de intentar remediar e informa del incumplimiento.

Para dejar espacio para que Firewall Manager lleve a cabo sus actividades de corrección, puede solicitar un aumento del límite. Como alternativa, puede cambiar la configuración de la política o la ACL de la red para reducir el número de reglas utilizadas.

Para obtener información sobre los límites de las ACL de la red, consulte las cuotas de Amazon VPC en las ACL de la red en la Guía del usuario de Amazon VPC.

Cuando se produce un error en la corrección

Al actualizar una ACL de red, si el Firewall Manager necesita detenerse por algún motivo, no revierte los cambios, sino que deja la ACL de la red en un estado provisional. Si ve reglas duplicadas en una ACL de red que tiene la `FMManaged` etiqueta configurada en`true`, lo más probable es que Firewall Manager esté solucionando el problema. Es posible que los cambios se hayan completado parcialmente durante un período, pero debido al enfoque que adopta Firewall Manager para solucionarlos, esto no interrumpirá el tráfico ni reducirá la protección de las subredes asociadas.

Cuando Firewall Manager no corrige por completo las ACL de red que no cumplen con los requisitos, informa del incumplimiento de las subredes asociadas y sugiere posibles opciones de corrección.

Al volver a intentarlo una vez se produce un error en la corrección

En la mayoría de los casos, si Firewall Manager no completa los cambios de corrección en una ACL de red, eventualmente volverá a intentar el cambio.

La excepción a esto ocurre cuando la corrección alcanza el límite de recuento de reglas de ACL de la red o el límite de recuento de ACL de la red de la VPC. Firewall Manager no puede realizar actividades de corrección que consuman AWS recursos por encima de su configuración límite. En estos casos, es necesario reducir los recuentos o aumentar los límites para poder continuar. Para obtener información sobre los límites, consulte las cuotas de Amazon VPC en las ACL de red en la Guía del usuario de Amazon VPC.

Informes de cumplimiento de ACL de red de Firewall Manager

Firewall Manager supervisa e informa del cumplimiento de todas las ACL de red que están conectadas a las subredes incluidas en el ámbito de aplicación.

En términos generales, el incumplimiento se produce en situaciones como un orden incorrecto de las reglas o un conflicto en el comportamiento de gestión del tráfico entre las reglas de política y las reglas personalizadas. Los informes de incumplimiento incluyen las infracciones de conformidad y las opciones de remediación.

Firewall Manager informa sobre las infracciones de conformidad de una política de ACL de red de la misma manera que para otros tipos de políticas. Para obtener información sobre los informes de conformidad, consulteVisualización de la información de cumplimiento de una AWS Firewall Manager política.

Incumplimiento durante las actualizaciones de las políticas

Después de modificar una política de ACL de red, hasta que Firewall Manager actualice las ACL de red que están dentro del ámbito de la política, Firewall Manager marca esas ACL de red como no conformes. Firewall Manager lo hace incluso si las ACL de la red pueden, estrictamente hablando, cumplir con las normas.

Por ejemplo, si elimina las reglas de la especificación de la política y las ACL de red incluidas en el ámbito de aplicación siguen teniendo reglas adicionales, es posible que sus definiciones de reglas sigan cumpliendo con la política. Sin embargo, dado que las reglas adicionales forman parte de las reglas que administra Firewall Manager, Firewall Manager las considera infracciones de la configuración de políticas actual. Esto es diferente de la forma en que el Administrador de Firewall ve las reglas personalizadas que se agregan a las ACL de red administradas por Firewall Manager.

Mejores prácticas para usar las políticas de ACL de red de Firewall Manager

En esta sección se enumeran las recomendaciones para trabajar con las políticas de ACL de red y las ACL de red administradas de Firewall Manager.

Consulte la **FMManaged** etiqueta para identificar las ACL de red administradas por Firewall Manager

Las ACL de red que administra Firewall Manager tienen la `FMManaged` etiqueta configurada en. `true` Use esta etiqueta para distinguir sus propias ACL de red personalizadas de las que administra mediante Firewall Manager.

No modifique el valor de la **FMManaged** etiqueta en una ACL de red

Firewall Manager usa esta etiqueta para establecer y determinar su estado de administración con una ACL de red.

No modifique las asociaciones de las subredes que tienen ACL de red administradas por Firewall Manager

No cambie manualmente las asociaciones entre las subredes y las ACL de red administradas por Firewall Manager. Si lo hace, puede inhabilitar la capacidad del Firewall Manager para administrar las protecciones de esas subredes. Puede identificar las ACL de red administradas por el Firewall Manager consultando la configuración de `FMManaged` etiquetas de`true`.

Para eliminar una subred de la administración de políticas del Firewall Manager, utilice la configuración del ámbito de la política del Firewall Manager para excluir la subred. Por ejemplo, puede etiquetar la subred y, a continuación, excluirla del ámbito de la política. Para obtener más información, consulte AWS Firewall Manager alcance de la política.

Cuando actualice una ACL de red administrada, no modifique las reglas que administra Firewall Manager

En una ACL de red administrada por Firewall Manager, mantenga sus reglas personalizadas separadas de las reglas de política siguiendo el esquema de numeración descrito en. Reglas y etiquetado de ACL de red de Firewall Manager Agregue o modifique únicamente las reglas que tengan números entre 5000 y 32 000.

Evita añadir demasiadas reglas a los límites de tu cuenta

Durante la corrección de una ACL de red, el Firewall Manager suele aumentar temporalmente el recuento de reglas de ACL de la red. Para evitar problemas de incumplimiento, asegúrese de tener suficiente espacio para las reglas que utilice. Para obtener más información, consulte Cómo corrige Firewall Manager las ACL de red gestionadas que no cumplen las normas.

Comience con la corrección automática desactivada

Comience con la corrección automática deshabilitada y, a continuación, revise la información detallada de la política para determinar los efectos que tendría la corrección automática. Cuando esté convencido de que los cambios son lo que desea, edite la política y habilite la corrección automática.

Advertencias sobre la política de ACL de red de Firewall Manager

En esta sección se enumeran las advertencias y limitaciones relacionadas con el uso de las políticas de ACL de red de Firewall Manager.

- Tiempos de actualización más lentos que con otras políticas: Firewall Manager suele aplicar las políticas de ACL de red y los cambios de política con más lentitud que con otras políticas de Firewall Manager, debido a las limitaciones en la velocidad a la que las API de ACL de red de Amazon EC2 pueden procesar las solicitudes. Es posible que observe que los cambios de política tardan más que los cambios similares con otras políticas del Firewall Manager, especialmente cuando agrega una política por primera vez.
- Para la protección inicial de subredes, Firewall Manager prefiere las políticas más antiguas. Esto solo se aplica a las subredes que aún no están protegidas por una política de ACL de red de Firewall Manager. Si una subred entra en el ámbito de aplicación de más de una política de ACL de red al mismo tiempo, Firewall Manager utiliza la política más antigua para proteger la subred.
- Motivos por los que una política deja de proteger una subred: una política que administra la ACL de red de una subred conserva la administración hasta que ocurra una de las siguientes situaciones:
  - La subred queda fuera del ámbito de aplicación de la política.
  - Se elimina la política.
  - La asociación de la subred se cambia manualmente a una ACL de red que se administra mediante una política de Firewall Manager diferente y cuyo ámbito de aplicación es la subred.

Eliminar una política de ACL de red de Firewall Manager

Al eliminar una política de ACL de red de Firewall Manager, Firewall Manager cambia los valores de las `FMManaged` etiquetas a `false` los de todas las ACL de red que ha estado administrando para la política.

Además, puede elegir si desea limpiar los recursos creados por la política. Si elige limpiar, el Firewall Manager intentará realizar los siguientes pasos en orden:

1. Vuelva a colocar la asociación en la original: Firewall Manager intenta volver a asociar la subred a la ACL de red a la que estaba asociada antes de que Firewall Manager comenzara a administrarla.
2. Eliminar la primera y la última regla de la ACL de la red: si no puede cambiar la asociación, el Firewall Manager intenta eliminar la primera y la última regla de la política, dejando solo las reglas personalizadas en la ACL de la red que está asociada a la subred.
3. No altere las reglas ni la asociación: si no puede hacer ninguna de las cosas anteriores, Firewall Manager deja la ACL de la red y su asociación tal como están.

Si no elige la opción de limpieza, tendrá que administrar manualmente cada ACL de la red después de eliminar la política. En la mayoría de las situaciones, elegir la opción de eliminación es el enfoque más sencillo.

AWS Network Firewall políticas

Puede usar las políticas de AWS Firewall Manager Network Firewall para administrar los AWS Network Firewall firewalls de sus VPC de Amazon Virtual Private Cloud en toda su organización en. AWS Organizations Puede aplicar firewalls controlados centralmente a toda su organización o a un subconjunto selecto de sus cuentas y VPC.

Network Firewall proporciona protecciones de filtrado de tráfico de red para las subredes públicas de sus VPC. Firewall Manager crea y administra sus firewalls en función del tipo de administración de firewall definido por su política. Firewall Manager proporciona los siguientes modelos de administración de firewall:

- Distribuido: para cada cuenta y VPC que se encuentra dentro del alcance de la política, Firewall Manager crea un firewall de Network Firewall e implementa puntos de conexión de firewall en las subredes de VPC para filtrar el tráfico de la red.
- Centralizado: Firewall Manager crea un único firewall de Network Firewall en una única Amazon VPC.
- Importar firewalls existentes: Firewall Manager importa los firewalls existentes para su administración en una única política de Firewall Manager. Puede aplicar reglas adicionales a los firewalls importados administrados por su política para asegurarse de que cumplen con sus estándares de seguridad.

> **Note**
>
> Las políticas de Firewall Manager Network Firewall son políticas de Firewall Manager que se utilizan para administrar las protecciones del Firewall de red para las VPC de toda su organización.
> Las protecciones de Network Firewall se especifican en los recursos del servicio Network Firewall que se denominan políticas de firewall.

Para obtener más información sobre Network Firewall, consulte la Guía para desarrolladores de AWS Network Firewall.

En las siguientes secciones se describen los requisitos para utilizar las políticas de Firewall Manager Network Firewall y se describe su funcionamiento. Para conocer el procedimiento para crear la política, consulte Crear una AWS Firewall Manager política para AWS Network Firewall.

Debe habilitar el uso compartido de recursos

Una política de Network Firewall comparte los grupos de reglas de Network Firewall entre las cuentas de su organización. Para que esto funcione, debe tener activado el uso compartido de recursos para AWS Organizations. Para obtener información acerca de cómo habilitar el uso compartido de recursos, consulte Uso compartido de recursos para las políticas de Network Firewall y DNS Firewall.

Debe tener definidos sus grupos de reglas de Network Firewall

Cuando especifica una nueva política de Network Firewall, define la política de firewall de la misma manera que cuando la usa AWS Network Firewall directamente. Especifique los grupos de reglas sin estado que desea agregar, las acciones sin estado predeterminadas y los grupos de reglas con estado. Sus grupos de reglas deben existir ya en la cuenta de administrador del Firewall Manager para que pueda incluirlos en la política. Para obtener información sobre cómo crear grupos de reglas de Network Firewall, consulte Grupos de reglas de AWS Network Firewall.

Cómo crea Firewall Manager los puntos de conexión del firewall

El tipo de administración de firewall de su política determina la forma en que Firewall Manager crea los firewalls. Su política puede crear firewalls distribuidos, un firewall centralizado o puede importar firewalls existentes:

- Distributed: con el modelo de implementación distribuida, Firewall Manager crea puntos de conexión en cada VPC que se encuentre dentro del alcance de la política. Puede personalizar

la ubicación de los puntos de conexión especificando en qué zonas de disponibilidad desea crear puntos de conexión del firewall, o Firewall Manager puede crear puntos de conexión automáticamente en las zonas de disponibilidad con subredes públicas. Si selecciona manualmente las zonas de disponibilidad, tiene la opción de restringir el conjunto de CIDR permitidos por zona de disponibilidad. Si decide permitir que Firewall Manager cree automáticamente los puntos de conexión, también debe especificar si el servicio va a crear un único punto de conexión o varios puntos de conexión de firewall dentro de sus VPC.

- Para varios puntos de conexión de firewall, Firewall Manager implementa un punto de conexión de firewall en cada zona de disponibilidad en la que tenga una subred con una puerta de enlace de Internet o una ruta de punto de conexión de firewall creada por Firewall Manager en la tabla de enrutamiento. Esta es la opción predeterminada para una política de Network Firewall.
- Para un único punto de conexión de firewall, Firewall Manager implementa un punto de conexión de firewall en una sola zona de disponibilidad en cualquier subred que tenga una ruta de puerta de enlace de Internet. Con esta opción, el tráfico en otras zonas debe cruzar los límites de la zona para que el firewall lo filtre.

> **Note**
>
> Para ambas opciones, debe haber una subred asociada a una tabla de enrutamiento que contenga una ruta IPv4/PrefixList. Firewall Manager no comprueba si hay otros recursos.

- Centralizado: con el modelo de implementación centralizada, Firewall Manager crea uno o más puntos de conexión de firewall dentro de una VPC de inspección. Una VPC de inspección es una VPC central en la que Firewall Manager lanza sus puntos de conexión. Cuando utiliza el modelo de implementación centralizada, también especifica en qué zonas de disponibilidad desea crear puntos de conexión de firewall. No puede cambiar la VPC de inspección después de crear su política. Para usar una VPC de inspección distinta, debe crear una política nueva.
- Importar firewalls existentes: al importar firewalls existentes, elija los firewalls que desea administrar en su política agregando uno o más conjuntos de recursos a su política. Un conjunto de recursos es una colección de recursos, en este caso firewalls existentes en Network Firewall, que son administrados por una cuenta de su organización. Antes de utilizar conjuntos de recursos en la política, primero debe crear un conjunto de recursos. Para obtener información sobre los conjuntos de recursos de Firewall Manager, consulte Trabajar con conjuntos de recursos en Firewall Manager.

  Tenga en cuenta las siguientes consideraciones al trabajar con firewalls importados:

- Si un firewall importado deja de ser compatible, Firewall Manager intentará resolver automáticamente la infracción, excepto en las siguientes circunstancias:
  - Si no coinciden las acciones predeterminadas con o sin estado de la política de Firewall Manager y Network Firewall.
  - Si un grupo de reglas de la política de firewall de un firewall importado tiene la misma prioridad que un grupo de reglas de la política de Firewall Manager.
  - Si un firewall importado usa una política de firewall asociada a un firewall, esa política no forma parte del conjunto de recursos de la política. Esto puede suceder porque un firewall puede tener exactamente una política de firewall, pero una única política de firewall puede estar asociada a varios firewalls.
  - Si se asigna una prioridad diferente a un grupo de reglas preexistente que pertenece a la política de firewall de un firewall importado y que también se especifica en la política del Firewall Manager.
- Si habilita la limpieza de recursos en la política, el Firewall Manager elimina los grupos de reglas que han estado en la política de importación de FMS de los firewalls dentro del alcance del conjunto de recursos.
- Los firewalls administrados por un Firewall Manager importan el tipo de administración de firewall existente solo pueden ser administrados por una política a la vez. Si se agrega el mismo conjunto de recursos a varias políticas de importación de firewalls de red, los firewalls del conjunto de recursos serán administrados por la primera política a la que se agregó el conjunto de recursos y serán ignorados por la segunda política.
- Actualmente, Firewall Manager no transmite configuraciones de políticas de excepción. Para obtener información sobre las políticas de excepciones de transmisión, consulte la Política de excepción de transmisión) en la Guía para desarrolladores de AWS Network Firewall .

Si cambia la lista de zonas de disponibilidad para las políticas que utilizan una administración de firewall distribuida o centralizada, Firewall Manager intentará limpiar todos los puntos de conexión que se hayan creado en el pasado, pero que actualmente no estén dentro del alcance de la política. Firewall Manager eliminará el punto de conexión solo si no hay rutas de la tabla de enrutamiento que hagan referencia al punto de conexión fuera del alcance. Si Firewall Manager descubre que no puede eliminar estos puntos de conexión, marcará la subred del firewall como no compatible y seguirá intentando eliminar el punto de conexión hasta que sea seguro eliminarlo.

Cómo administra Firewall Manager sus subredes de firewall

Las subredes de firewall son las subredes de VPC que Firewall Manager crea para los puntos de conexión de firewall que filtran el tráfico de su red. Cada punto de conexión de firewall debe implementarse en una subred de VPC dedicada. Firewall Manager crea al menos una subred de firewall en cada VPC que esté dentro del alcance de aplicación de la política.

Para las políticas que utilizan el modelo de implementación distribuida con configuración automática de puntos de conexión, Firewall Manager solo crea subredes de firewall en las zonas de disponibilidad que tienen una subred con una ruta de puerta de enlace de Internet o una subred con una ruta a los puntos de conexión de firewall que Firewall Manager creó para su política. Para obtener más información, consulte VPC y subredes en la Guía del usuario de Amazon VPC.

Para las políticas que utilizan el modelo distribuido o centralizado, en el que se especifican las zonas de disponibilidad en las que el Firewall Manager crea los puntos de conexión del firewall, Firewall Manager crea un punto de conexión en esas zonas de disponibilidad específicas, independientemente de si hay otros recursos en la zona de disponibilidad.

Al definir por primera vez una política de un Firewall de red, se especifica la forma en que Firewall Manager administra las subredes del firewall en cada una de las VPC que están dentro del alcance. No podrá cambiar esta opción más adelante.

En el caso de las políticas que utilizan el modelo de implementación distribuido con una configuración automática de puntos de conexión, puede elegir entre las siguientes opciones:

- Implemente una subred de firewall para cada zona de disponibilidad que tenga subredes públicas. Este es el comportamiento predeterminado. Esto proporciona una alta disponibilidad de sus protecciones de filtrado de tráfico.
- Implemente una única subred de firewall en una zona de disponibilidad. Con esta opción, Firewall Manager identifica una zona de la VPC que tiene mayor cantidad de subredes públicas y crea la subred de firewall allí. El único punto de conexión del firewall filtra todo el tráfico de red para la VPC. Esto puede reducir los costos del firewall, pero no tiene alta disponibilidad y requiere que el tráfico de otras zonas cruce los límites de la zona para poder ser filtrado.

Para las políticas que utilizan un modelo de implementación distribuido con una configuración de punto de conexión personalizada o el modelo de implementación centralizado, Firewall Manager crea las subredes en las zonas de disponibilidad especificadas que se encuentran dentro del alcance de la política.

Puede proporcionar bloques CIDR de VPC para que Firewall Manager los utilice en las subredes del firewall o puede dejar que Firewall Manager determine la elección de las direcciones de punto de conexión del firewall.

- Si no proporciona bloques CIDR, Firewall Manager consulta las direcciones IP disponibles en sus VPC para utilizarlas.
- Si proporciona una lista de bloques de CIDR, el Firewall Manager busca nuevas subredes solo en los bloques de CIDR que proporcione. Debe usar bloques CIDR de /28. Para cada subred de firewall que crea Firewall Manager, recorre su lista de bloques de CIDR y usa la primera que encuentra que es aplicable a la zona de disponibilidad y a la VPC y que tiene direcciones disponibles. Si Firewall Manager no puede encontrar espacios abiertos en la VPC (con o sin la restricción), el servicio no creará un firewall en la VPC.

Si Firewall Manager no puede crear una subred de firewall requerida en una zona de disponibilidad, marca la subred como no compatible con la política. Mientras la zona se encuentre en este estado, el tráfico de la zona debe cruzar los límites de la zona para que un punto de conexión de otra zona pueda filtrarlo. Esto es similar al escenario de una única subred de firewall.

Cómo administra Firewall Manager sus recursos de Network Firewall

Al definir la política en el Firewall Manager, se proporciona el comportamiento de filtrado del tráfico de red de una política de AWS Network Firewall firewall estándar. Puede agregar grupos de reglas de Network Firewall sin estado y con estado y especificar las acciones predeterminadas para los paquetes que no coincidan con ninguna regla sin estado. Para obtener información sobre cómo trabajar con las políticas de firewall AWS Network Firewall, consulte las políticas de AWS Network Firewall firewall.

Para políticas distribuidas y centralizadas, cuando guarde la política de Network Firewall, Firewall Manager crea un firewall y una política de firewall en cada VPC que esté dentro del alcance de la política. Firewall Manager asigna un nombre a estos recursos de Network Firewall mediante la concatenación de los siguientes valores:

- Una cadena fija, `FMManagedNetworkFirewall` o bien `FMManagedNetworkFirewallPolicy`, según el tipo de recurso.
- Nombre de la política de Firewall Manager. Es el nombre que asigna al crear la política.
- ID de la política de Firewall Manager. Este es el ID AWS de recurso de la política del Firewall Manager.

- ID de Amazon VPC. Este es el ID AWS de recurso de la VPC en la que Firewall Manager crea el firewall y la política de firewall.

A continuación se muestra un nombre de ejemplo para un firewall administrado por Firewall Manager:

```
FMManagedNetworkFirewallEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

A continuación se muestra un ejemplo de nombre de política de firewall:

```
FMManagedNetworkFirewallPolicyEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

Después de crear la política, las cuentas de los miembros en las VPC no pueden anular la configuración de su política de firewall ni sus grupos de reglas, pero pueden añadir grupos de reglas a la política de firewall que ha creado Firewall Manager.

Cómo Firewall Manager administra y supervisa las tablas de enrutamiento de VPC para su política

> **Note**
>
> Actualmente, la administración de tablas de enrutamiento no es compatible con las políticas que utilizan el modelo de implementación centralizada.

Cuando Firewall Manager crea los puntos de conexión del firewall, también crea las tablas de enrutamiento de VPC para ellos. Sin embargo, Firewall Manager no administra las tablas de enrutamiento de la VPC. Debe configurar las tablas de enrutamiento de la VPC para dirigir el tráfico de red a los puntos de conexión del firewall creados por Firewall Manager. Con las mejoras de enrutamiento de ingreso de Amazon VPC, cambie las tablas de enrutamiento para enrutar el tráfico a través de los nuevos puntos de conexión del firewall. Los cambios deben insertar los puntos de conexión del firewall entre las subredes que desea proteger y las ubicaciones externas. El enrutamiento exacto que debe realizar depende de su arquitectura y sus componentes.

Actualmente, Firewall Manager permite supervisar las rutas de la tabla de enrutamiento de la VPC para detectar cualquier tráfico destinado a la puerta de enlace de Internet, es decir, que esté eludiendo el firewall. Firewall Manager no admite otras puertas de enlace de destino, como las puertas de enlace NAT.

Para obtener información sobre la administración de las tablas de enrutamiento de la VPC, consulte Administrar las tablas de enrutamiento de su VPC en la Guía del usuario de Amazon Virtual Private

Cloud. Para obtener información sobre la administración de las tablas de enrutamiento para Network Firewall, consulte Configuraciones de tablas de enrutamiento de AWS Network Firewall en la Guía para desarrolladores de AWS Network Firewall .

Cuando habilita la supervisión de una política, Firewall Manager supervisa continuamente las configuraciones de rutas de la VPC y le alerta sobre el tráfico que elude la inspección del firewall de esa VPC. Si una subred tiene una ruta de punto de conexión de firewall, Firewall Manager busca las siguientes rutas:

- Rutas para enviar el tráfico al punto de conexión de Network Firewall.
- Rutas para reenviar el tráfico desde el punto de conexión de Network Firewall a la puerta de enlace de Internet.
- Rutas entrantes desde la puerta de enlace de Internet al punto de conexión de Network Firewall.
- Rutas desde la subred del firewall.

Si una subred tiene una ruta de Network Firewall, pero hay un enrutamiento asimétrico en el Firewall de red y en la tabla de enrutamiento de la puerta de enlace de Internet, Firewall Manager informa que la subred no es compatible. Firewall Manager también detecta las rutas a la puerta de enlace de Internet en la tabla de enrutamiento del firewall que creó Firewall Manager, así como en la tabla de enrutamiento de la subred, y las informa como no compatibles. Las rutas adicionales de la tabla de enrutamiento de subred de Network Firewall y la tabla de enrutamiento de la puerta de enlace de Internet también se reportan como no compatibles. Según el tipo de infracción, Firewall Manager sugiere acciones correctivas para que la configuración de la ruta cumpla con las normas. Firewall Manager no ofrece sugerencias en todos los casos. Por ejemplo, si la subred de su cliente tiene un punto de conexión de firewall que se creó fuera de Firewall Manager, Firewall Manager no sugiere acciones correctivas.

De forma predeterminada, Firewall Manager marcará cualquier tráfico que cruce el límite de la zona de disponibilidad para su inspección como no compatible. Sin embargo, si decide crear automáticamente un punto de conexión único en su VPC, Firewall Manager no marcará el tráfico que cruce el límite de la zona de disponibilidad como no compatible.

En el caso de las políticas que utilizan modelos de implementación distribuidos con una configuración de punto de conexión personalizada, puede elegir si el tráfico que cruza el límite de la zona de disponibilidad desde una zona de disponibilidad sin un punto de conexión de firewall se marca como compatible o no.

> **Note**
>
> - Firewall Manager no sugiere acciones correctivas para las rutas que no son IPv4, como IPv6 y las rutas de lista de prefijos.
> - Las llamadas realizadas mediante la llamada a la API `DisassociateRouteTable` pueden demorar hasta 12 horas en detectarse.
> - Firewall Manager crea una tabla de enrutamiento de Network Firewall para una subred que contiene los puntos de conexión del firewall. Firewall Manager asume que esta tabla de enrutamiento contiene solo rutas de puerta de enlace de Internet válidas y rutas predeterminadas de VPC. Cualquier ruta adicional o no válida de esta tabla de enrutamiento se considera no compatible.

Cuando configura su política de Firewall Manager, si elige el modo Supervisar, Firewall Manager proporciona detalles sobre las infracciones de recursos y las correcciones relacionadas con sus recursos. Puede utilizar estas acciones correctivas sugeridas para solucionar problemas de enrutamiento en sus tablas de enrutamiento. Si selecciona el modo Desactivado, Firewall Manager no supervisa el contenido de la tabla de enrutamiento por usted. Con esta opción, puede administrar las tablas de enrutamiento de VPC. Para obtener más información acerca de estas infracciones de recursos, consulte Visualización de la información de cumplimiento de una AWS Firewall Manager política.

> **Warning**
>
> Si selecciona Supervisar en la configuración de AWS Network Firewall rutas al crear la política, no podrá desactivarla para esa política. Sin embargo, si elige Desactivar, podrás habilitarla más adelante.

Configurar el registro para una AWS Network Firewall política

Puede habilitar el registro centralizado para sus políticas de Network Firewall para obtener información detallada sobre el tráfico dentro de su organización. Puede seleccionar el registro de flujo para capturar el flujo de tráfico de la red o el registro de alertas para informar del tráfico que coincide con una regla con la acción de la regla establecida en `DROP` o en `ALERT`. Para obtener más información sobre el registro de AWS Network Firewall , consulte Registro del tráfico de red desde AWS Network Firewall en la Guía para desarrolladores de AWS Network Firewall .

Envíe los registros desde los firewalls de Network Firewall de su política a un bucket de Amazon S3. Después de habilitar el registro, AWS Network Firewall entrega los registros de cada Network Firewall configurado actualizando la configuración del firewall para entregar los registros a los buckets de Amazon S3 seleccionados con el AWS Firewall Manager prefijo reservado,. `<policy-name>-<policy-id>`

> **Note**
>
> Firewall Manager utiliza este prefijo para determinar si Firewall Manager agregó una configuración de registro o si la agregó el propietario de la cuenta. Si el propietario de la cuenta intenta usar el prefijo reservado para su propio registro personalizado, la configuración de registro de la política del Firewall Manager lo sobrescribe.

Para obtener más información sobre cómo crear un bucket de Amazon S3 y revisar los registros almacenados, consulte ¿Qué es Amazon S3? en la Guía del usuario de Amazon Simple Storage Service.

Para habilitar el registro, debe cumplir con los siguientes requisitos:

- El Amazon S3 que especifique en su política de Firewall Manager debe existir.
- Debe tener los siguientes permisos:
  - `logs:CreateLogDelivery`
  - `s3:GetBucketPolicy`
  - `s3:PutBucketPolicy`
- Si el bucket de Amazon S3 que es su destino de registro utiliza cifrado del lado del servidor con claves almacenadas en él AWS Key Management Service, debe añadir la siguiente política a la clave AWS KMS gestionada por el cliente para permitir que Firewall Manager inicie sesión en su CloudWatch grupo de registros:

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt*",
```

```
            "kms:Decrypt*",
            "kms:ReEncrypt*",
            "kms:GenerateDataKey*",
            "kms:Describe*"
        ],
        "Resource": "*"
}
```

Tenga en cuenta que solo los buckets de la cuenta de administrador del Firewall Manager se pueden usar para el registro de AWS Network Firewall centralizado.

Cuando habilita el registro centralizado en una política de Network Firewall, Firewall Manager realiza las siguientes acciones en su cuenta:

- Firewall Manager actualiza los permisos en los buckets S3 seleccionados para permitir la entrega de registros.
- Firewall Manager crea directorios en el bucket de S3 para cada cuenta de miembro dentro del alcance de la política. Los registros de cada cuenta se encuentran en `<bucket-name>/<policy-name>-<policy-id>/AWSLogs/<account-id>`.

Habilitación del registro de una política de Network Firewall

1. Cree un bucket de Amazon S3 con la cuenta de administrador de Firewall Manager. Para obtener más información, consulte Creación de un bucket en la Guía del usuario de Amazon Simple Storage Service.
2. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

3. En el panel de navegación, seleccione Políticas de Seguridad.

4. Elija la política de Network Firewall para la que desea habilitar el registro. Para obtener más información sobre el AWS Network Firewall registro, consulte Registrar el tráfico de red AWS Network Firewall en la Guía para AWS Network Firewall desarrolladores.
5. En la pestaña Detalles de la política, en la sección Reglas de la política, seleccione Editar.
6. Para habilitar y agregar registros, seleccione una o más opciones en Configuración de registros:
   - Habilite y agregue los registros de flujo
   - Habilite y agregue los registros de alertas
7. Elija el bucket de Amazon S3 en el que desea que se entreguen sus registros. Debe elegir un bucket para cada tipo de registro que active. Puede usar el mismo bucket para ambos tipos de registros.
8. (Opcional) Si desea que el registro personalizado creado por la cuenta de un miembro se sustituya por la configuración de registro de la política, seleccione Anular la configuración de registro existente.
9. Elija Siguiente.
10. Revise su configuración y, a continuación, seleccione Guardar para guardar los cambios en la política.

Deshabilitación del registro de una política de Network Firewall

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Políticas de Seguridad.
3. Elija la política de Network Firewall para la que desea deshabilitar el registro.
4. En la pestaña Detalles de la política, en la sección Reglas de la política, seleccione Editar.
5. En el estado de la configuración del registro, quite la selección Habilitar y agregar registros de flujo y Habilitar y agregar registros de alertas si están seleccionadas.

6. Elija Siguiente.
7. Revise su configuración y, a continuación, seleccione Guardar para guardar los cambios en la política.

Políticas de DNS firewall de Amazon Route 53 Resolver

Puede utilizar las políticas de firewall de AWS Firewall Manager DNS para administrar las asociaciones entre los grupos de reglas de firewall de DNS de Amazon Route 53 Resolver y sus VPC de Amazon Virtual Private Cloud en toda la organización en AWS Organizations. Puede aplicar grupos de reglas controlados centralmente a toda su organización o a un subconjunto selecto de sus cuentas y VPC.

DNS Firewall proporciona filtrado y regulación del tráfico DNS saliente para sus VPC. Crea colecciones reutilizables de reglas de filtrado en grupos de reglas de DNS Firewall y asocia los grupos de reglas a sus VPC. Al aplicar la política de Firewall Manager para cada cuenta y VPC que se encuentra dentro del alcance de la política, Firewall Manager crea una asociación entre cada grupo de reglas de DNS firewall en la política y cada VPC que se encuentra dentro del alcance de la política, utilizando la configuración de prioridad de asociación que especifique en la política de Firewall Manager.

Para obtener información sobre el uso de DNS Firewall, consulte DNS Firewall de Amazon Route 53 Resolver, en la Guía para desarrolladores de Amazon Route 53.

En las siguientes secciones se describen los requisitos para usar las políticas de DNS firewall de Firewall Manager y se describe cómo funcionan las políticas. Para conocer el procedimiento para crear la política, consulte Creación de una AWS Firewall Manager política para Amazon Route 53 Resolver DNS Firewall.

Debe habilitar el uso compartido de recursos

Una política de DNS firewall comparte los grupos de reglas de DNS firewall entre las cuentas de su organización. Para que esto funcione, debe tener activado el uso compartido de recursos con AWS Organizations. Para obtener información acerca de cómo habilitar el uso compartido de recursos, consulte Uso compartido de recursos para las políticas de Network Firewall y DNS Firewall.

Debe tener definidos los grupos de reglas de DNS Firewall

Cuando especifica una nueva política de DNS firewall, define los grupos de reglas de la misma manera que cuando utiliza directamente el DNS firewall de Amazon Route 53 Resolver. Sus grupos

de reglas deben existir ya en la cuenta de administrador del Firewall Manager para que pueda incluirlos en la política. Para obtener información sobre la creación de grupos de reglas del DNS Firewall, consulte Reglas y grupos de reglas de DNS Firewall.

Defina las asociaciones de grupos de reglas de prioridad más baja y más alta

Las asociaciones de grupos de reglas de DNS Firewall que administra mediante las políticas de Firewall Manager de DNS Firewall contienen las asociaciones de menor prioridad y las asociaciones de mayor prioridad para sus VPC. En la configuración de políticas, aparecen como primer y último grupo de reglas.

DNS firewall filtra el tráfico de DNS de la VPC en el siguiente orden:

1. Primeros grupos de reglas, definidos por usted en la política de DNS Firewall Manager. Los valores válidos se encuentran entre 1 y 99.
2. Grupos de reglas de DNS firewall que los administradores de cuentas individuales asocian a través del DNS firewall.
3. Últimos grupos de reglas, definidos por usted en la política de DNS Firewall Manager. Los valores válidos están entre 9.901 y 10.000.

Eliminar un grupo de reglas

Para eliminar un grupo de reglas de una política DNS firewall de Firewall Manager, debe realizar los siguientes pasos:

1. Elimine el grupo de reglas de la política de DNS Firewall Manager.
2. Deje de compartir el grupo de reglas en. AWS Resource Access Manager Para dejar de compartir un grupo de reglas de su propiedad, debe quitarlo del recurso compartido. Puede hacerlo mediante la AWS RAM consola o la AWS CLI. Para obtener más información sobre como dejar de compartir un recurso, consulte Actualizar un recurso compartido en AWS RAM en la Guía del usuario de AWS RAM .
3. Elimine el grupo de reglas mediante la consola del firewall DNS o la AWS CLI.

Cómo nombra Firewall Manager las asociaciones de grupos de reglas que crea

Al guardar la política de firewall de DNS, si ha habilitado la corrección automática, Firewall Manager crea una asociación de DNS firewall entre los grupos de reglas que proporcionó en la política y

las VPC que están dentro del alcance de la política. Firewall Manager nombra estas asociaciones concatenando los siguientes valores:

- La cadena fija, `FMManaged_`.
- ID de la política de Firewall Manager. Este es el ID AWS de recurso de la política del Firewall Manager.

A continuación se muestra un nombre de ejemplo para un firewall administrado por Firewall Manager:

```
FMManaged_EXAMPLEDNSFirewallPolicyId
```

Tras crear la política, si los propietarios de las cuentas de las VPC anulan la configuración de su política de firewall o las asociaciones de su grupo de reglas, Firewall Manager marcará la política como no compatible e intentará proponer una acción correctiva. Los propietarios de las cuentas pueden asociar otros grupos de reglas de DNS firewall a las VPC que estén dentro del alcance de la política de DNS firewall. Cualquier asociación creada por los propietarios de cuentas individuales debe tener una configuración de prioridad entre la primera y la última asociación del grupo de reglas.

Políticas de NGFW en la nube de Palo Alto Networks

El firewall de próxima generación (NGFW) en la nube de Palo Alto Networks es un servicio de firewall de terceros que puede utilizar para sus AWS Firewall Manager políticas. Con el NGFW en Cloud de Palo Alto Networks para Firewall Manager, puede crear e implementar de forma centralizada los recursos y conjuntos de reglas de NGFW en la nube de Palo Alto Networks en todas sus cuentas. AWS

Para utilizar el NGFW en la nube de Palo Alto Networks con Firewall Manager, primero debe suscribirse al servicio Pay-As-You-Go de Palo Alto Networks Cloud NGFW en Marketplace. AWS Después de suscribirse, debe realizar una serie de pasos en el servicio de NGFW en la nube de Palo Alto Networks para configurar su cuenta y los ajustes de NGFW en la nube. A continuación, debe crear una política de Firewall Manager Cloud FMS para implementar y gestionar de forma centralizada los recursos y las reglas de NGFW de Palo Alto Networks Cloud en todas las cuentas de sus organizaciones. AWS

Para obtener información sobre el procedimiento de creación de la política de Firewall Manager, consulte Creación de una AWS Firewall Manager política para el NGFW en la nube de Palo Alto Networks. Para obtener información sobre cómo configurar y administrar NGFW en la nube de Palo

Alto Networks para Firewall Manager, consulte la documentación de NGFW en la nube de Palo Alto Networks en AWS.

Políticas de Fortigate Cloud Native Firewall (CNF) como servicio

El firewall nativo en la nube (CNF) de Fortigate como servicio es un servicio de firewall de terceros que puede usar para sus AWS Firewall Manager políticas. Fortigate CNF es un servicio de firewall de última generación que le facilita la protección de sus redes en la nube y la administración de sus políticas de seguridad. Con Fortigate CNF para Firewall Manager, puede crear e implementar de forma centralizada los recursos y conjuntos de políticas de Fortigate CNF en todas sus cuentas. AWS

Para usar Fortigate CNF con Firewall Manager, primero debe suscribirse al Firewall nativo de Fortigate Cloud (CNF) como servicio en el Marketplace. AWS Después de suscribirse, debe realizar una serie de pasos en el servicio de Fortigate CNF para configurar sus conjuntos de políticas globales y otros ajustes. Luego, crea una política de Firewall Manager para implementar y administrar de forma centralizada los recursos de Fortigate CNF en todas las cuentas de sus Organizaciones AWS .

Para conocer el procedimiento de creación de una política de Fortigate CNF Firewall Manager, consulte Crear una AWS Firewall Manager política para Fortigate Cloud Native Firewall (CNF) como servicio. Para obtener información sobre cómo configurar y administrar Fortigate CNF para su uso con Firewall Manager, consulte la documentación de Fortigate CNF.

Uso compartido de recursos para las políticas de Network Firewall y DNS Firewall

Para administrar las políticas de Firewall Manager, Network Firewall y DNS Firewall, debe habilitar el uso compartido de recursos con AWS Organizations in AWS Resource Access Manager. Esto permite que Firewall Manager implemente protecciones en sus cuentas cuando cree estos tipos de políticas.

Para habilitar el uso compartido de recursos, siga las instrucciones que aparecen en Habilitación del uso compartido con AWS Organizations en la AWS Resource Access Manager Guía del usuario.

Problemas con el uso compartido de recursos

Es posible que tenga problemas con el uso AWS RAM compartido de recursos, ya sea cuando lo habilite o cuando esté trabajando en las políticas del Firewall Manager que lo requieren.

A continuación, se muestran ejemplos de estos problemas:

- Si sigue las instrucciones para habilitar el uso compartido, en la AWS RAM consola, la opción Habilitar el uso compartido con AWS Organizations aparece atenuada y no se puede seleccionar.
- Cuando trabaja en Firewall Manager en una política que requiere el uso compartido de recursos, la política se marca como no compatible y ve mensajes que indican que el uso compartido de recursos o AWS RAM no está habilitado.

Si tiene problemas con el uso compartido de recursos, use el siguiente procedimiento para intentar habilitarlo.

Vuelva a intentar habilitar el uso compartido de recursos

- Vuelva a intentar habilitar el uso compartido utilizando una de las siguientes opciones:
  - (Opcional) A través de la AWS RAM consola, sigue las instrucciones que aparecen en la Guía del AWS Resource Access Manager usuario, que se encuentran AWS Organizations en la sección Habilitar el uso compartido con.
  - (Opción) Con la AWS RAM API, llama`EnableSharingWithAwsOrganization`. Consulte la documentación en EnableSharingWithAwsOrganization.

Trabajar con conjuntos de recursos en Firewall Manager

Un conjunto de AWS Firewall Manager recursos es un conjunto de recursos, como firewalls, que puede agrupar y administrar en una política de Firewall Manager. Los conjuntos de recursos permiten a los miembros de su organización tener un control pormenorizado sobre los recursos que deben administrar en una política. Para usar conjuntos de recursos, cree un conjunto de recursos en la consola o mediante la PutResourceSetAPI y, a continuación, añada el conjunto de recursos a la política de Firewall Manager.

Puede crear y administrar conjuntos de recursos para los siguientes tipos de políticas de recursos y seguridad:

Tipo de recurso	Tipo de política de seguridad de Firewall Manager
AWS Network Firewall - firewalls	Política de Network Firewall: utilice conjuntos de recursos para importar los firewalls existente s desde Network Firewall. Para obtener información sobre el uso de conjuntos de recursos en una política de Network Firewall, consulte el paso Importar firewalls existentes del procedimiento de Crear una AWS Firewall Manager política para AWS Network Firewall.

En las siguientes secciones se describen los requisitos para crear y eliminar conjuntos de recursos.

Temas

Consideraciones al trabajar con conjuntos de recursos en Firewall Manager

Tenga en cuenta las siguientes consideraciones cuando trabaje con conjuntos de recursos

Referencias a recursos inexistentes

Cuando se añade un recurso a un conjunto de recursos, se crea una referencia al recurso con un nombre de recurso de Amazon (ARN). Firewall Manager valida que el nombre de recurso de Amazon (ARN) tenga el formato correcto, pero Firewall Manager no comprueba que el recurso al que se hace referencia exista. Si el recurso aún no existe y pasa la validación del ARN, Firewall Manager incluye la referencia del recurso en el conjunto de recursos. Si posteriormente se crea un nuevo recurso con el mismo ARN, Firewall Manager aplica los grupos de reglas de la política asociada al conjunto de recursos al nuevo recurso.

Recursos eliminados

Cuando se elimina un recurso de un conjunto de recursos, la referencia al recurso permanece en el conjunto de recursos hasta que el administrador del Firewall Manager la elimine.

Recursos propiedad de la cuenta de un miembro que abandona la organización AWS Organizations

Si una cuenta de miembro abandona la organización, todas las referencias a los recursos que sean propiedad de esa cuenta de miembro permanecerán en el conjunto de recursos, pero ya no se administrarán mediante ninguna política a la que esté asociado el conjunto de recursos.

Asociación a varias políticas

Un conjunto de recursos se puede asociar a varias políticas, pero no todos los tipos de políticas admiten varias políticas que administren el mismo recurso. Consulte la documentación correspondiente a su tipo de política específico para obtener información sobre los escenarios no admitidos.

Creación de los conjuntos de recursos

Cómo crear un conjunto de recursos (consola)

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, elija Recursos.

3. Elija Crear recurso compartido de recursos.
4. En Nombre del conjunto de recursos, escriba un nombre descriptivo.
5. (Opcional) introduzca una Descripción para el conjunto de recursos.
6. Elija Siguiente.
7. En Elegir recursos, seleccione un identificador de cuenta de AWS y, a continuación, seleccione Elegir recursos para añadir al conjunto de recursos los recursos que son propiedad de esta cuenta y están gestionados por ella. Después de seleccionar los recursos, seleccione Añadir para agregar los recursos al conjunto de recursos.
8. Elija Siguiente.
9. En el caso de las etiquetas del conjunto de recursos, añada las etiquetas de identificación que desee para el conjunto de recursos. Para obtener más información sobre etiquetas, consulte Trabajar con Tag Editor.
10. Elija Siguiente.
11. Revise el nuevo conjunto de recursos. Para realizar cualquier cambio, elija Editar en el área que desea cambiar. Esto le devuelve al paso correspondiente del asistente de creación. Cuando esté satisfecho con el conjunto de recursos, elija Crear conjunto de recursos.

Eliminación de de un conjunto de recursos

Antes de poder eliminar un conjunto de recursos, el conjunto de recursos debe estar disociado de todas las políticas que utilizan el conjunto de recursos. Puede desasociar los grupos de recursos en la página de detalles de la política mediante la consola o la PutPolicyAPI.

Eliminación de un conjunto de recursos (consola)

1. En el panel de navegación, elija Recursos.
2. Elija la opción situada junto al recurso que desea eliminar.
3. Elija Eliminar.

Visualización de la información de cumplimiento de una AWS Firewall Manager política

En esta sección se proporciona una guía para ver el estado de conformidad de las cuentas y los recursos que entran en el ámbito de aplicación de una AWS Firewall Manager política. Para obtener

información sobre los controles implementados AWS para mantener la seguridad y el cumplimiento de la nube, consulte[Validación de la conformidad en Firewall Manager](#).

> **Note**
>
> Para que Firewall Manager supervise el cumplimiento de las políticas, AWS Config debe registrar continuamente los cambios de configuración de los recursos protegidos. En su AWS Config configuración, la frecuencia de grabación debe estar establecida en Continua, que es la configuración predeterminada.

> **Note**
>
> Para mantener un estado de conformidad adecuado en sus recursos protegidos, evite cambiar repetidamente el estado de las protecciones del Firewall Manager, ya sea automática o manualmente. Firewall Manager utiliza la información de AWS Config para detectar cambios en las configuraciones de los recursos. Si los cambios se aplican con la suficiente rapidez, se AWS Config puede perder la pista de algunos de ellos, lo que puede provocar la pérdida de información sobre el cumplimiento o el estado de corrección en Firewall Manager.
>
> Si ve que un recurso que está protegiendo con Firewall Manager tiene un estado de conformidad o corrección incorrecto, primero asegúrese de que no está ejecutando ningún proceso que altere o restablezca las protecciones de Firewall Manager y, a continuación, actualice el AWS Config seguimiento del recurso reevaluando las reglas de configuración asociadas en. AWS Config

Para todas AWS Firewall Manager las políticas, puede ver el estado de conformidad de las cuentas y los recursos que están dentro del ámbito de aplicación de la política. Una cuenta o un recurso cumple con una política de Firewall Manager si la configuración de la política se refleja en la configuración de la cuenta o el recurso. Cada tipo de política tiene sus propios requisitos de conformidad, que puede ajustar al definir la política. En el caso de algunas políticas, también puede ver información detallada sobre las infracciones en los recursos incluidos en el ámbito de aplicación, que le ayudarán a comprender y gestionar mejor los riesgos de seguridad.

Cómo visualizar la información de conformidad de una política

1. Inicie sesión AWS Management Console con su cuenta de administrador de Firewall Manager y, a continuación, abra la consola de Firewall Manager enhttps://console.aws.amazon.com/wafv2/fmsv2. Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

   > **Note**
   >
   > Para obtener información acerca de la configuración de una cuenta de administrador de Firewall Manager, consulte AWS Firewall Manager requisitos previos.

2. En el panel de navegación, seleccione Security policies (Políticas de seguridad).
3. Elija una política. En la pestaña Cuentas y recursos de la página de políticas, Firewall Manager muestra las cuentas de su organización, agrupadas por las que se encuentran dentro del ámbito de la política y las que se encuentran fuera de dicho ámbito.

   En el panel Cuentas dentro del ámbito de la política se muestra el estado de conformidad de cada cuenta. Un estado Conforme indica que la política se ha aplicado correctamente a todos los recursos dentro de su ámbito de la cuenta. Un estado No conforme indica que la política no se ha aplicado a uno más recursos dentro de su ámbito de la cuenta.
4. Elija una cuenta que no sea conforme. En la página de la cuenta, Firewall Manager muestra el identificador y el tipo de cada recurso no conforme y el motivo por el que el recurso infringe la política.

   > **Note**
   >
   > Para los tipos de recursos `AWS::EC2::NetworkInterface` (ENI) y `AWS::EC2::Instance`, Firewall Manager podría mostrar un número limitado de recursos no conformes. Para enumerar otros recursos no conformes, corrija los que se muestran inicialmente para la cuenta.

5. Si el tipo de política de Firewall Manager es una política de grupo de seguridad de auditoría de contenido, puede acceder a la información detallada sobre las infracciones de un recurso.

   Para ver los detalles sobre la infracción, elija el recurso.

> **Note**
>
> Es posible que los recursos no conformes que Firewall Manager encuentre antes de añadir la página detallada sobre infracciones de recursos no tengan detalles sobre infracciones.

En la página de recursos, Firewall Manager muestra detalles específicos sobre la infracción, según el tipo de recurso.

- **`AWS::EC2::NetworkInterface`** (ENI): Firewall Manager muestra información sobre el grupo de seguridad que el recurso no cumple. Elija el grupo de seguridad para ver más detalles sobre él.
- **`AWS::EC2::Instance`**: Firewall Manager muestra el ENI asociado a la instancia de EC2 que no es compatible. También muestra información sobre el grupo de seguridad que los recursos no cumplen. Elija el grupo de seguridad para ver más detalles sobre él.
- **`AWS::EC2::SecurityGroup`**: Firewall Manager muestra los siguientes detalles de infracción:
  - Regla de grupo de seguridad no conforme: la regla que causa la infracción, incluidos su protocolo, rango de puertos, rango de IP CIDR y descripción.
  - Regla referenciada: la regla del grupo de seguridad de auditoría que infringe la regla del grupo de seguridad no conforme, con sus detalles.
  - Motivos de la infracción: explicación del resultado no conforme.
  - Acción correctiva: la acción que se sugiere tomar. Si Firewall Manager no puede determinar una acción correctiva segura, este campo está en blanco.
- **`AWS::EC2::Subnet`**— Se utiliza para las políticas de ACL de red y Network Firewall.

  Firewall Manager muestra el ID de subred, el ID de VPC y la zona de disponibilidad.
  Si corresponde, Firewall Manager incluye información adicional sobre la infracción. El componente de descripción de la infracción contiene una descripción del estado esperado del recurso, el estado actual de no conformidad y, si está disponible, una descripción de la causa de la discrepancia.

  Violaciones de Network Firewall

- Infracciones en la administración de rutas: en el caso de las políticas de Network Firewall que utilizan el modo Monitor, Firewall Manager muestra información básica de subred, así como las rutas esperadas y reales de la subred, la puerta de enlace de Internet y la tabla de enrutamiento de subred de Network Firewall. Firewall Manager le avisa de que existe una infracción si las rutas reales no coinciden con las rutas esperadas en la tabla de enrutamiento.
- Acciones correctivas en caso de infracciones en la administración de rutas: en el caso de las políticas de Network Firewall que utilizan el modo Monitor, Firewall Manager sugiere posibles acciones correctivas en las configuraciones de rutas que contengan infracciones.

Por ejemplo, supongamos que se espera que una subred envíe tráfico a través de los puntos finales del firewall, pero la subred actual envía tráfico directamente a la puerta de enlace de Internet. Se trata de una infracción de la administración de rutas. La corrección sugerida en este caso podría ser una lista de acciones ordenadas. La primera es la recomendación de agregar las rutas necesarias a la tabla de enrutamiento de la subred de Firewall Network para dirigir el tráfico saliente a la puerta de enlace de Internet y el tráfico entrante para los destinos en la VPC hacia `local`. La segunda recomendación es reemplazar la ruta de la puerta de enlace de Internet o la ruta no válida de Network Firewall en la tabla de enrutamiento de la subred para dirigir el tráfico saliente a los puntos de conexión del firewall. La tercera recomendación consiste en agregar las rutas necesarias a la tabla de enrutamiento de la puerta de enlace de Internet para dirigir el tráfico entrante a los puntos de conexión del firewall.

- **`AWS::EC2::InternetGateway`**: se usa para las políticas de Network Firewall que tienen habilitado el modo Monitor.
  - Infracciones en la administración de rutas: la puerta de enlace de Internet no es conforme si no está asociada a una tabla de enrutamiento o si hay una ruta no válida en la tabla de enrutamiento de la puerta de enlace de Internet.
  - Acciones correctivas en caso de infracciones en la administración de rutas: Firewall Manager sugiere posibles acciones correctivas para subsanar las infracciones en la administración de rutas.

Example 1. Infracción en la administración de rutas y sugerencias de corrección

Una puerta de enlace de Internet no está asociada a una tabla de enrutamiento. Las acciones de corrección sugeridas podrían ser una lista de acciones ordenadas. La primera acción es crear una tabla de enrutamiento. La segunda acción es asociar la tabla de enrutamiento con la

puerta de enlace de Internet. La tercera acción consiste en añadir la ruta requerida a la tabla de enrutamiento de la puerta de enlace de Internet.

Example 2. Infracción en la administración de rutas y sugerencias de corrección

La puerta de enlace de Internet está asociada a una tabla de enrutamiento válida, pero la ruta no está configurada correctamente. La corrección sugerida podría ser una lista de acciones ordenadas. La primera sugerencia es eliminar la ruta no válida. La tercera consiste en agregar la ruta requerida a la tabla de enrutamiento de la puerta de enlace de Internet.

- **`AWS::NetworkFirewall::FirewallPolicy`**: se utiliza para las políticas de Network Firewall. Firewall Manager muestra información sobre una política de firewall de Network Firewall que se ha modificado de forma que no sea conforme. La información proporciona la política de firewall esperada y la política que encontró en la cuenta del cliente, de modo que puede comparar los nombres de los grupos de reglas sin y con estado y las configuraciones de prioridad, los nombres de las acciones personalizadas y la configuración predeterminada de las acciones sin estado. El componente de descripción de la infracción contiene una descripción del estado esperado del recurso, el estado actual de no conformidad y, si está disponible, una descripción de la causa de la discrepancia.
- **`AWS::EC2::VPC`**: se utiliza para las políticas de DNS Firewall. Firewall Manager muestra información sobre una VPC que está dentro del ámbito de aplicación de una política de DNS Firewall de Firewall Manager y que no la cumple. La información proporcionada incluye los grupos de reglas esperadas que se espera que estén asociadas a la VPC y los propios grupos de reglas. El componente de descripción de la infracción contiene una descripción del estado esperado del recurso, el estado actual de no conformidad y, si está disponible, una descripción de la causa de la discrepancia.

AWS Firewall Manager hallazgos

AWS Firewall Manager obtiene información sobre los recursos que no cumplen con las normas y sobre los ataques que detecta y a los que los envía AWS Security Hub. Para obtener información sobre los resultados de Security Hub, consulte, Resultados en AWS Security Hub.

Cuando usa Security Hub y Firewall Manager, Firewall Manager envía automáticamente sus resultados a Security Hub. Para obtener información acerca de cómo comenzar a usar , consulte Configuración de AWS Security Hub en la Guía del usuario de AWS Security Hub.

> **Note**
>
> Firewall Manager solo actualiza los resultados de las políticas que administra y de los recursos que supervisa.
> Firewall Manager no resuelve los siguientes problemas:
>
> - Políticas que se han eliminado.
> - Recursos que se han eliminado.
> - Recursos que han quedado fuera del ámbito de aplicación de la política del Firewall Manager, por ejemplo, debido a un cambio en la etiqueta o en la definición de la política.

¿Cómo se pueden consultar los resultados del Firewall Manager?

Para ver sus resultados de Firewall Manager en Security Hub, siga la orientación de Uso de resultados en Security Hub y cree un filtro con la configuración siguiente:

- Atributo establecido en Nombre de producto.
- Operador establecido en EQUALS.
- Valor establecido en `Firewall Manager`. Esta configuración distingue entre mayúsculas y minúsculas.

¿Puedo desactivar esto?

Puede deshabilitar la integración de los AWS Firewall Manager hallazgos con el Security Hub a través de la consola de Security Hub. Elija Integraciones en la barra de navegación y, a continuación, en el panel de Firewall Manager, elija Deshabilitar integración. Para obtener más información, consulte la Guía del usuario de AWS Security Hub.

AWS Firewall Manager tipos de búsqueda

- AWS WAF hallazgos de políticas
- AWS Shield Advanced hallazgos de políticas
- Resultados de la política común del grupo de seguridad
- Resultados de política de auditoría de contenido del grupo de seguridad
- Resultados de política de auditoría de uso del grupo de seguridad
- Resultados de la política de DNS Firewall de Amazon Route 53 Resolver

AWS WAF hallazgos de políticas

Puede usar AWS WAF las políticas del Firewall Manager para aplicar grupos de AWS WAF reglas a sus recursos en AWS Organizations. Para obtener más información, consulte Trabajar con AWS Firewall Manager políticas.

Falta la ACL web administrada por Firewall Manager.

Un AWS recurso no tiene la asociación de ACL web AWS Firewall Manager gestionada de acuerdo con la política del Firewall Manager. Puede habilitar la corrección de Firewall Manager en la política para corregir esto.

- Gravedad: 80
- Configuración de estado: APROBADO/FALLIDO
- Actualizaciones: si Firewall Manager realiza la acción correctiva, actualizará el resultado y la gravedad disminuirá de `HIGH` a `INFORMATIONAL`. Si realiza la corrección, Firewall Manager no actualizará el resultado.

La ACL web administrada por Firewall Manager tiene grupos de reglas configurados incorrectamente.

Los grupos de reglas en una ACL web que está administrada por Firewall Manager no están configurados correctamente, de acuerdo con la política de . Esto significa que en la ACL web faltan los grupos de reglas que la política requiere. Puede habilitar la corrección de Firewall Manager en la política para corregir esto.

- Gravedad: 80
- Configuración de estado: APROBADO/FALLIDO
- Actualizaciones: si Firewall Manager realiza la acción correctiva, actualizará el resultado y la gravedad disminuirá de `HIGH` a `INFORMATIONAL`. Si realiza la corrección, Firewall Manager no actualizará el resultado.

AWS Shield Advanced hallazgos de políticas

Para obtener información sobre AWS Shield Advanced las políticas, consultePolíticas de grupos de seguridad.

El recurso carece de la protección Shield Advanced.

Un AWS recurso que debería tener la protección Shield Advanced, de acuerdo con la política del Firewall Manager, no la tiene. Puede habilitar la corrección de Firewall Manager en la política, lo que habilitará la protección del recurso.

- Gravedad: 60
- Configuración de estado: APROBADO/FALLIDO
- Actualizaciones: si Firewall Manager realiza la acción correctiva, actualizará el resultado y la gravedad disminuirá de `HIGH` a `INFORMATIONAL`. Si realiza la corrección, Firewall Manager no actualizará el resultado.

Shield Advanced ha detectado un ataque contra el recurso monitorizado.

Shield Advanced ha detectado un ataque a un AWS recurso protegido. Puede habilitar la corrección de Firewall Manager en la política.

- Gravedad: 70
- Configuración de estado: ninguna
- Actualizaciones: Firewall Manager no actualiza este resultado.

Resultados de la política común del grupo de seguridad

Para obtener información sobre las políticas comunes de grupo de seguridad, consulte Políticas de grupos de seguridad.

El recurso ha configurado incorrectamente el grupo de seguridad.

Firewall Manager ha identificado un recurso al que le faltan las asociaciones de grupo de seguridad administradas por Firewall Manager que debería tener, según la política de Firewall Manager. Puede habilitar la corrección de Firewall Manager en la política, lo que crea las asociaciones según las opciones de la política.

- Gravedad: 70
- Configuración de estado: APROBADO/FALLIDO
- Actualizaciones: Firewall Manager actualiza este resultado.

La réplica de grupo de seguridad de Firewall Manager no está sincronizada con el grupo de seguridad principal.

Una réplica de grupo de seguridad de Firewall Manager no está sincronizada con su grupo de seguridad principal, según su política común de grupo de seguridad. Puede habilitar la corrección de Firewall Manager en la política, lo que sincronizará los grupos de seguridad de réplica con el principal.

- Gravedad: 80
- Configuración de estado: APROBADO/FALLIDO
- Actualizaciones: Firewall Manager actualiza este resultado.

Resultados de política de auditoría de contenido del grupo de seguridad

Para obtener información sobre las políticas de auditoría de contenido del grupo de seguridad, consulte Políticas de grupos de seguridad.

El grupo de seguridad no es conforme con el grupo de seguridad de auditoría de contenido.

Una política de auditoría de contenido del grupo de seguridad de Firewall Manager ha identificado un grupo de seguridad que no es conforme. Se trata de un grupo de seguridad creado por el cliente que se encuentra en el ámbito de la política de auditoría de contenido y que no es conforme con la configuración definida por la política y su grupo de seguridad de auditoría. Puede habilitar la corrección de Firewall Manager en la política, lo que modifica el grupo de seguridad que no es conforme para que lo sea.

- Gravedad: 70
- Configuración de estado: APROBADO/FALLIDO
- Actualizaciones: Firewall Manager actualiza este resultado.

Resultados de política de auditoría de uso del grupo de seguridad

Para obtener información sobre las políticas de auditoría de uso del grupo de seguridad, consulte Políticas de grupos de seguridad.

Firewall Manager encontró un grupo de seguridad redundante.

La auditoría de uso del grupo de seguridad de Firewall Manager ha identificado un grupo de seguridad redundante. Se trata de un grupo de seguridad con un conjunto de reglas idénticas a las de otro grupo de seguridad en la misma instancia de Amazon Virtual Private Cloud. Puede habilitar

la corrección automática de Firewall Manager en la política de auditoría de uso, lo que reemplaza los grupos de seguridad redundantes por un único grupo de seguridad.

- Gravedad: 30
- Configuración de estado: ninguna
- Actualizaciones: Firewall Manager no actualiza este resultado.

Firewall Manager encontró un grupo de seguridad no utilizado.

La auditoría de uso del grupo de seguridad de Firewall Manager ha identificado un grupo de seguridad no usado. Se trata de un grupo de seguridad al que no hace referencia ninguna política común de grupo de seguridad de Firewall Manager. Puede habilitar la reparación automática de Firewall Manager en la política de auditoría de uso, lo que elimina los grupos de seguridad no utilizados.

- Gravedad: 30
- Configuración de estado: ninguna
- Actualizaciones: Firewall Manager no actualiza este resultado.

Resultados de la política de DNS Firewall de Amazon Route 53 Resolver

Para obtener más información sobre las políticas de DNS Firewall, consulte Políticas de DNS firewall de Amazon Route 53 Resolver.

Falta la protección del firewall de DNS en el recurso

A una VPC le falta una asociación de grupos de reglas de firewall de DNS definida en la política de firewall de DNS de Firewall Manager. El resultado muestra el grupo de reglas especificado por la política.

- Gravedad: 80

Seguridad en el uso del AWS Firewall Manager servicio

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

> **Note**
>
> Esta sección proporciona una guía de AWS seguridad estándar para el uso del AWS Firewall Manager servicio y sus AWS recursos, como las políticas de Firewall Manager Network Firewall y las políticas de grupos de seguridad.
> Para obtener información sobre cómo proteger sus AWS recursos mediante el Administrador de Firewall, consulte el resto de la guía del Administrador de Firewall.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad que se aplican a Firewall Manager, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Firewall Manager. En los siguientes temas, se le mostrará cómo configurar Firewall Manager para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger los recursos del Firewall Manager.

Temas

Protección de datos en Firewall Manager

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS Firewall Manager. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con el Firewall Manager u otro Servicios de AWS dispositivo mediante la consola, la API o AWS los SDK. AWS CLI Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los

registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Las entidades de Firewall Manager, como las políticas, se cifran en reposo, excepto en ciertas regiones donde el cifrado no está disponible, incluidas China (Pekín) y China (Ningxia). Para cada región se utilizan claves de cifrado únicas.

Identity and Access Management para AWS Firewall Manager

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede estar autenticado (iniciar sesión) y autorizado (tener permisos) para utilizar los recursos de Firewall Manager. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realice en Firewall Manager.

Usuario de servicio: si utiliza el servicio de Firewall Manager para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Firewall Manager para realizar su trabajo, es posible que necesite permisos

adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en Firewall Manager, consulte Solución de problemas AWS Shield de identidad y acceso.

Administrador de servicio: si está a cargo de los recursos de Firewall Manager en su empresa, probablemente tenga acceso completo a . Su trabajo consiste en determinar a qué características y recursos de Firewall Manager deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Firewall Manager, consulte Cómo AWS Shield funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a Firewall Manager . Para consultar ejemplos de políticas basadas en la identidad de Firewall Manager que puede utilizar en IAM, consulte Ejemplos de políticas basadas en identidades de AWS Shield.

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS Single Sign-On y Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios empresarial, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS Single Sign-On. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como

contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS Single Sign-On.
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.

- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un AWS rol a una instancia EC2 y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia

contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo

o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifique el usuario o rol en el

campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.

- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo AWS Firewall Manager funciona con IAM

Antes de utilizar IAM para administrar el acceso a Firewall Manager, conozca qué características de IAM se pueden utilizar con Firewall Manager .

Funciones de IAM que puede utilizar con AWS Firewall Manager

Característica de IAM	Soporte de Firewall Manager
Políticas basadas en identidades	Sí

Característica de IAM	Soporte de Firewall Manager
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	No
ACL	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Parcial
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan el Firewall Manager y otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidades para Firewall Manager

Compatibilidad con las políticas basadas en identidades	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Para ver ejemplos de políticas basadas en identidad de Firewall Manager, consulte Ejemplos de políticas basadas en la identidad para AWS Firewall Manager.

Ejemplos de políticas basadas en identidades para Firewall Manager

Para ver ejemplos de políticas basadas en identidad de Firewall Manager, consulte Ejemplos de políticas basadas en la identidad para AWS Firewall Manager.

Políticas basadas en recursos dentro de Firewall Manager

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a

una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Acciones de política en Firewall Manager

Admite acciones de política	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de Firewall Manager, consulte Acciones definidas por AWS Firewall Manager en la Referencia de autorizaciones de servicio.

Las acciones de política en Firewall Manager utilizan el prefijo siguiente antes de la acción:

```
fms
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "fms:action1",
      "fms:action2"
         ]
```

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

```
"Action": "fms:Describe*"
```

Para ver ejemplos de políticas basadas en identidad de Firewall Manager, consulte Ejemplos de políticas basadas en la identidad para AWS Firewall Manager.

Recursos de políticas en Firewall Manager

Admite recursos de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de recursos de Firewall Manager y sus ARN, consulte Recursos definidos por AWS Firewall Manager en la Referencia de autorizaciones de servicio. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Firewall Manager.

Para ver ejemplos de políticas basadas en identidad de Firewall Manager, consulte Ejemplos de políticas basadas en la identidad para AWS Firewall Manager.

Claves de condición para Firewall Manager

Admite claves de condición de políticas específicas del servicio	No

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación lógica `AND`. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de Firewall Manager, consulte Claves de condición para AWS Firewall Manager en la Referencia de autorizaciones de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por AWS Firewall Manager.

Para ver ejemplos de políticas basadas en identidad de Firewall Manager, consulte Ejemplos de políticas basadas en la identidad para AWS Firewall Manager.

Las ACL en Firewall Manager

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con Firewall Manager

Admite ABAC (etiquetas en las políticas)	Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Firewall Manager

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes

AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para Firewall Manager

Admite Forward access sessions (FAS)	Sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Rolescde servicio en Firewall Manager

Compatible con roles de servicio	Parcial

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Firewall Manager. Edite los roles de servicio solo cuando Firewall Manager proporcione orientación para hacerlo.

Elegir un rol de IAM en Firewall Manager

Para usar la acción de *PutNotificationChannel*API en Firewall Manager, debe elegir un rol que permita que Firewall Manager acceda a Amazon SNS para que el servicio pueda publicar los mensajes de Amazon SNS en su nombre. Para obtener más información, consulte la referencia PutNotificationChannelde la AWS Firewall Manager API.

A continuación se muestra un ejemplo de configuración de permisos de tema SNS. Para usar esta política con su rol personalizado, sustituya el nombre de recurso de Amazon (ARN) `AWSServiceRoleForFMS` por `SnsRoleName` ARN.

```
{
  "Sid": "AWSFirewallManagerSNSPolicy",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account ID:role/aws-service-role/
fms.amazonaws.com/AWSServiceRoleForFMS"
  },
  "Action": "sns:Publish",
  "Resource": "SNS topic ARN"
}
```

Para obtener más información sobre las acciones y los recursos del Firewall Manager, consulte el tema de la AWS Identity and Access Management guía Acciones definidas por AWS Firewall Manager

Roles vinculados a servicios de Firewall Manager

Compatible con roles vinculados al servicio	Sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio

aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya Yes en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en la identidad para AWS Firewall Manager

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de Firewall Manager. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

A fin de obtener más información sobre las acciones y los tipos de recursos definidos por Firewall Manager, incluido el formato de los ARN para cada tipo de recurso, consulte Acciones, recursos y claves de condición para AWS Firewall Manager en la Referencia de autorizaciones de servicio.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola de Firewall Manager
- Cómo permitir a los usuarios consultar sus propios permisos
- Otorgue acceso de lectura a sus grupos de seguridad de Firewall Manager

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Firewall Manager de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola de Firewall Manager

Para acceder a la AWS Firewall Manager consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle registrar y consultar los detalles acerca de los recursos de Firewall Manager en su Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y las funciones puedan seguir utilizando la consola del Firewall Manager, adjunte también el Firewall Manager *ConsoleAccess* o la política *ReadOnly* AWS gestionada a las entidades. Para más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Otorgue acceso de lectura a sus grupos de seguridad de Firewall Manager

Firewall Manager permite el acceso a recursos de varias cuentas, pero no permite crear protecciones de recursos de varias cuentas. Solo puede crear protecciones para los recursos desde la cuenta que posee esos recursos.

A continuación, se muestra un ejemplo de política que concede permisos para las acciones `fms:Get`, `fms:List` y `ec2:DescribeSecurityGroups` en todos los recursos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "fms:Get*",
                "fms:List*",
                "ec2:DescribeSecurityGroups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS políticas gestionadas para AWS Firewall Manager

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS política gestionada: **`AWSFMAdminFullAccess`**

Utilice la política `AWSFMAdminFullAccess` AWS gestionada para permitir a los administradores acceder a los AWS Firewall Manager recursos, incluidos todos los tipos de políticas del Firewall Manager. Esta política no incluye los permisos para configurar las notificaciones del Amazon Simple Notification Service en AWS Firewall Manager. Para obtener información sobre cómo configurar el acceso a Amazon Simple Notification Service, consulte Configuración del acceso para Amazon SNS.

Para ver la lista y los detalles de las políticas, consulte la consola de IAM en AWSFMAdminFullAccess. El resto de esta sección ofrece una descripción general de la configuración de las políticas.

Declaraciones de permiso

Esta política se agrupa en instrucciones basadas en el conjunto de permisos.

- AWS Firewall Manager recursos de políticas: permite permisos administrativos completos a los recursos AWS Firewall Manager, incluidos todos los tipos de políticas de Firewall Manager.
- Escribir AWS WAF registros en Amazon Simple Storage Service: permite que Firewall Manager escriba y lea AWS WAF registros en Amazon S3.

- Crear rol vinculado al servicio: permite al administrador crear un rol vinculado al servicio, que permite que Firewall Manager analice los recursos de otros servicios en su nombre. Este permiso permite crear el rol vinculado a servicios solo para su uso por Firewall Manager. Para obtener más información acerca de cómo utiliza Firewall Manager los roles vinculados a servicios, consulte Uso de roles vinculados a servicios para Firewall Manager.
- AWS Organizations: Permite a los administradores utilizar Firewall Manager para una organización en AWS Organizations. Tras habilitar el acceso de confianza para Firewall Manager en AWS Organizations, los miembros de la cuenta de administrador pueden ver los resultados de su organización. Para obtener información sobre su uso AWS Organizations con AWS Firewall Manager, consulte Uso AWS Organizations con otros AWS servicios en la Guía del AWS Organizations usuario.

Categorías de permisos

A continuación, se enumeran los tipos de permisos de la política y los permisos que proporcionan.

- `fms`— Trabaje con AWS Firewall Manager los recursos.
- `wafy waf-regional` — Trabaje con políticas AWS WAF clásicas.
- `elasticloadbalancing`— Asocie las ACL AWS WAF web a los Elastic Load Balancers.
- `firehose`— Ver información sobre los registros. AWS WAF
- `organizations`— Trabaja con los recursos de AWS Organizations.
- `shield`— Ver el estado de AWS Shield las políticas de suscripción.
- `route53resolver`— Trabaje con los grupos de reglas de DNS privado para VPC de Route 53 en una política de DNS privado para VPC de Route 53.
- `wafv2`— Trabaje con políticas AWS WAFV2 .
- `network-firewall`— Trabajar con AWS Network Firewall políticas.
- `ec2`— Ver las zonas y regiones de disponibilidad de la política.
- `s3`— Ver información sobre AWS WAF los registros.

AWS política gestionada: **`FMSServiceRolePolicy`**

Esta política le permite AWS Firewall Manager administrar AWS los recursos en su nombre en el Firewall Manager y en los servicios integrados. Esta política se adjunta al rol vinculado al servicio de `AWSServiceRoleForFMS`. Para obtener más información sobre el rol vinculado a servicios, consulte Uso de roles vinculados a servicios para Firewall Manager.

Para obtener información detallada sobre la política, consulte la consola de IAM en ServiceRolePolicyFMS.

AWS política gestionada: AWSFMAdminReadOnlyAccess

Otorga acceso de solo lectura a todos los recursos del AWS Firewall Manager.

Para ver la lista de políticas y los detalles, consulte la consola de IAM en. AWSFMAdminReadOnlyAccess El resto de esta sección ofrece una descripción general de la configuración de las políticas.

Categorías de permisos

A continuación, se enumeran los tipos de permisos de la política y la información a la que los permisos permiten el acceso de solo lectura.

- `fms`— AWS Firewall Manager recursos.
- `wafy waf-regional` — Políticas AWS WAF clásicas.
- `firehose`— AWS WAF registros.
- `organizations`— Recursos de AWS Organizations.
- `shield`— AWS Shield políticas.
- `route53resolver`— Grupos de reglas de DNS privado para VPC de Route 53 en una política de DNS privado para VPC de Route 53.
- `wafv2`— Sus grupos de AWS WAFV2 reglas y los grupos de reglas de reglas AWS administradas que están disponibles en. AWS WAFV2
- `network-firewall`— grupos de AWS Network Firewall reglas y metadatos de grupos de reglas.
- `ec2`— AWS Network Firewall políticas, zonas y regiones de disponibilidad.
- `s3`— AWS WAF registros.

AWS política gestionada: AWSFMMemberReadOnlyAccess

Otorga acceso de solo lectura a los recursos de los AWS Firewall Manager miembros. Para ver la lista de políticas y los detalles, consulte la consola de IAM en. AWSFMMemberReadOnlyAccess

Firewall Manager actualiza las políticas AWS administradas

Vea los detalles sobre las actualizaciones de las políticas AWS administradas para Firewall Manager desde que este servicio comenzó a rastrear estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos en Historial de documentos.

Cambio	Descripción	Fecha
FMS ServiceRolePolicy: política actualizada	Se agregaron permisos para administrar las ACL de la red. Consulte la política actualizada en la consola de IAM: FMS.ServiceRolePolicy	22 de abril de 2020
FMS — Política actualizada ServiceRolePolicy	Se agregaron permisos que permiten al Firewall Manager describir si las AWS Config reglas especificadas son compatibles. Consulte la política actualizada en la consola de IAM: ServiceRolePolicyFMS.	21 de abril de 2021
FMS — Política actualizada ServiceRolePolicy	Se añadieron permisos que permiten a Firewall Manager describir los atributos de la interfaz de red y la instancia de Amazon EC2. Consulte la política actualizada en la consola de IAM: FMS.ServiceRolePolicy	15-11-2022
AWSFMAdminReadOnlyAccess: política actualizada	Se han añadido permisos para admitir AWS WAFV2	2022-11-02

Cambio	Descripción	Fecha
	políticas como Shield, Network Firewall, DNS Firewall, grupo de seguridad Amazon VPC. Consulte la política actualizada en la consola de IAM:. AWSFMAdminReadOnlyAccess	
AWSFMAdminFullAccess: política actualizada	Se han añadido permisos para admitir AWS WAFV2 políticas como Shield, Network Firewall, DNS Firewall, grupo de seguridad Amazon VPC. Se eliminaron los permisos de Amazon SNS. Consulte la política actualizada en la consola de IAM:. AWSFMAdminFullAccess	2022-10-21
`FMSServiceRolePolicy` — Nuevos permisos para las políticas de firewall de terceros AWS Firewall Manager	Este cambio permite a Firewall Manager crear y eliminar los puntos de enlace de VPC de Amazon EC2 asociados a una política de firewall de terceros.	30 de marzo de 2022

Cambio	Descripción	Fecha
`FMSServiceRolePolicy` — Nuevos permisos para las políticas AWS Network Firewall	Se agregaron nuevos permisos para admitir la implementación de firewalls para las políticas de Network Firewall. Los nuevos permisos permiten recuperar información sobre las zonas de disponibilidad para las cuentas que están incluidas en el ámbito de aplicación de una política.	2022-02-16
`FMSServiceRolePolicy` — Nuevos permisos para las políticas AWS Shield	Se agregaron nuevos permisos para recuperar etiquetas de recursos AWS WAF regionales y AWS WAF globales. Se agregaron permisos AWS WAF regionales para recuperar las ACL web mediante un ARN de recurso. Se agregaron permisos para admitir la mitigación automática de DDoS en la capa de aplicaciones de Shield.	07/01/2022
`FMSServiceRolePolicy` — Nuevos permisos para las políticas AWS Shield	Se agregó un nuevo permiso para recuperar etiquetas para los recursos de equilibrador de carga.	18-11-2021

Cambio	Descripción	Fecha
`FMSServiceRolePolicy` — Nuevos permisos para grupos y políticas de seguridad AWS Network Firewall	Se agregaron nuevos permisos para permitir el registro centralizado de AWS Network Firewall las políticas . Además, se agregaron permisos de Amazon EC2 de solo lectura para admitir los cambios en el servicio Config que afectan a la forma en que se AWS Firewall Manager consultan los recursos para las políticas de los grupos de seguridad.	29 de septiembre de 2021
`FMSServiceRolePolicy` — Formatos ARN para recursos AWS WAF	Se actualizó `FMSServiceRolePolicy` para estandarizar los formatos ARN de los recursos de AWS WAF . Los formatos ARN actualizados son `arn:aws:waf:*:*:*` y `arn:aws:waf-regional:*:*:*` .	2021-08-12
`FMSServiceRolePolicy` : regiones adicionales en China	AWS Firewall Manager se ha habilitado `FMSServiceRolePolicy` para las regiones BJS y ZHY de China.	2021-08-12

Cambio	Descripción	Fecha
`FMSServiceRolePolicy` : actualización de la política actual	Se agregaron nuevos permisos para permitir administrar Amazon Route 53 Resolver el firewall AWS Firewall Manager de DNS. Este cambio permite a Firewall Manager configurar las asociaciones de firewall de Amazon Route 53 Resolver DNS. Esto le permite usar Firewall Manager para proporcionar protecciones de firewall de DNS para sus VPC en toda la organización en AWS Organizations.	-17 de marzo de 2021
Firewall Manager comenzó a realizar el seguimiento de los cambios	Firewall Manager comenzó a rastrear los cambios de sus políticas AWS administradas.	02-03-02

Solución de problemas AWS Firewall Manager de identidad y acceso

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Firewall Manager e IAM.

Temas

- No tengo autorización para realizar una acción en Firewall Manager
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a los recursos de mi Firewall Manager

No tengo autorización para realizar una acción en Firewall Manager

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `fms:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fms:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `fms:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a Firewall Manager.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM llamado `marymajor` intenta utilizar la consola para realizar una acción en Firewall Manager. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a los recursos de mi Firewall Manager

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para obtener información acerca de si Firewall Manager admite estas características, consulte Cómo AWS Shield funciona con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Uso de roles vinculados a servicios para Firewall Manager

AWS Firewall Manager utiliza funciones AWS Identity and Access Management vinculadas al servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Firewall Manager. El Firewall Manager predefine las funciones vinculadas al servicio e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado al servicio simplifica la configuración de Firewall Manager porque ya no tendrá que agregar manualmente los permisos requeridos. Firewall Manager define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Firewall Manager puede

asumir sus roles. Los permisos definidos incluyen la política de confianza y la política de permisos. Dicha política de permisos no se puede asociar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a un servicio después de eliminar los recursos relacionados del rol. De esta forma, se protegen los recursos de Firewall Manager, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a un servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Administración de permisos de roles vinculados a Firewall Manager

AWS Firewall Manager utiliza el nombre del rol vinculado al servicio AWSServiceRoleForFMS para permitir que Firewall Manager llame a AWS los servicios en su nombre para administrar las políticas de firewall y los recursos de la AWS Organizations cuenta. Esta política está asociada a la función AWS gestionada. `AWSServiceRoleForFMS` Para obtener más información sobre el rol administrado, consulte AWS política gestionada: `FMSServiceRolePolicy`.

El rol AWSServiceRoleForFMS vinculado al servicio confía en que el servicio lo asuma el rol. `fms.amazonaws.com`

La política de permisos del rol permite que Firewall Manager realice las siguientes acciones en los recursos especificados:

- `waf`- Administre las ACL web AWS WAF clásicas, los permisos de los grupos de reglas y las asociaciones de las ACL web en su cuenta.
- `ec2`: administre grupos de seguridad en interfaces de red elásticas e instancias de Amazon EC2. Gestione las ACL de red en las subredes de Amazon VPC.
- `vpc`: administre subredes, tablas de enrutamiento, etiquetas y puntos de enlace en Amazon VPC.
- `wafv2`- Administre las ACL AWS WAF web, los permisos de los grupos de reglas y las asociaciones de ACL web en su cuenta.
- `cloudfront`- Cree ACL web para proteger las distribuciones. CloudFront
- `config`- Administre las AWS Config reglas propiedad de Firewall Manager en su cuenta.
- `iam`- Gestione esta función vinculada al servicio y cree las funciones obligatorias y las vinculadas al servicio AWS WAF Shield si configura el registro y AWS WAF las políticas de Shield.

- `organization`- Cree un rol vinculado a un servicio propiedad de Firewall Manager para administrar AWS Organizations los recursos utilizados por Firewall Manager.
- `shield`- Gestione AWS Shield las protecciones y las configuraciones de mitigación L7 para los recursos de su cuenta.
- `ram`- Gestione el uso compartido de AWS RAM recursos para los grupos de reglas de DNS Firewall y los grupos de reglas de Network Firewall.
- `network-firewall`- Administre AWS Network Firewall los recursos propiedad de Firewall Manager y los recursos de Amazon VPC dependientes en su cuenta.
- `route53resolver`: administre las asociaciones de firewall DNS propiedad de Firewall Manager en su cuenta.

Consulte la política completa en la consola de IAM: FMS. ServiceRolePolicy

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio para Firewall Manager

No necesita crear manualmente un rol vinculado a servicios. Cuando habilita el AWS Management Console inicio de sesión de Firewall Manager o realiza una `PutLoggingConfiguration` solicitud en la CLI o la API de Firewall Manager, Firewall Manager crea el rol vinculado al servicio por usted.

Debe tener el permiso `iam:CreateServiceLinkedRole` para habilitar el registro.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al habilitar los registros de Firewall Manager, Firewall Manager se encarga de volver crear automáticamente el rol vinculado al servicio.

Edición de un rol vinculado a un servicio para Firewall Manager

Firewall Manager no le permite editar el rol AWSServiceRoleForFMS vinculado al servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio para Firewall Manager

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se monitorice ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el servicio de Firewall Manager está utilizando el rol cuando intenta eliminar los recursos, la eliminación podría producir un error. En tal caso, espere unos minutos e intente de nuevo la operación.

Eliminación del rol vinculado a servicios con IAM

Utilice la consola de IAM, la CLI de IAM o la API de IAM para eliminar el rol vinculado al AWSServiceRoleForFMS servicio. Para más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a servicios de Firewall Manager

Firewall Manager admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte Puntos de conexión y cuotas de Firewall Manager.

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar un confuso problema de diputado. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que lo ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Se recomienda utilizar las claves de contexto de condición `aws:SourceAccount`global `aws:SourceArn`y las claves de contexto en las políticas de recursos para limitar los permisos que

se AWS Firewall Manager otorgan a otro servicio al recurso. Utilice `aws:SourceArn` si desea que solo se asocie un recurso al acceso entre servicios. Utilice `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo del recurso o si está especificando varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con caracteres comodines (*) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:fms:*:`*`account-id`*`:*`.

Si el valor de `aws:SourceArn` no contiene el ID de cuenta, como un ARN de bucket de Amazon S3, debe utilizar ambas claves de contexto de condición global para limitar los permisos.

El valor de `aws:SourceArn` debe ser la AWS cuenta del AWS Firewall Manager administrador.

En los siguientes ejemplos se muestra cómo se puede utilizar la clave de contexto de condición global `aws:SourceArn` en Firewall Manager para evitar el problema del suplente confuso.

En el ejemplo siguiente se muestra cómo evitar el problema del suplente confuso usando la clave de contexto de condición global de `aws:SourceArn` en la política de confianza de rol de Firewall Manager. Sustituya *`region`* y *`account-id`* con su propia información.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "servicename.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": [
          "arn:aws:fms:Region:account-id:${*}",
          "arn:aws:fms:Region:account-id:policy/*"]
      },
      "StringEquals": {
        "aws:SourceAccount": "account-id"
      }
    }
  }
```

```
}
```

Registro y supervisión en Firewall Manager

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Firewall Manager y sus AWS soluciones. Debe recopilar los datos de supervisión de todas las partes de la AWS solución para poder depurar con mayor facilidad un error multipunto en caso de que se produzca. AWS proporciona varias herramientas para supervisar los recursos del Firewall Manager y responder a posibles eventos:

CloudWatch Alarmas Amazon

Al usar CloudWatch las alarmas, puede observar una única métrica durante un período de tiempo que especifique. Si la métrica supera un umbral determinado, CloudWatch envía una notificación a un tema o AWS Auto Scaling política de Amazon SNS. Para obtener más información, consulte Monitorización con Amazon CloudWatch.

AWS CloudTrail Registros

CloudTrail proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Firewall Manager. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó al Firewall Manager, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales. Para obtener más información, consulte Registro de llamadas a la API de AWS CloudTrail con.

Validación de la conformidad en Firewall Manager

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

  > **Note**
  >
  > No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos

de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.

- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en Firewall Manager

La infraestructura AWS global se basa en distintas zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Seguridad de la infraestructura en AWS Firewall Manager

Como servicio gestionado, AWS Firewall Manager está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Las llamadas a la API AWS publicadas se utilizan para acceder a Firewall Manager a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.

- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

AWS Firewall Manager cuotas

AWS Firewall Manager está sujeto a las siguientes cuotas (anteriormente denominadas límites).

AWS Firewall Manager tiene cuotas predeterminadas que puede aumentar y cuotas fijas.

Las políticas de grupos de seguridad y las políticas de ACL de red que administra Firewall Manager están sujetas a las cuotas estándar de Amazon VPC. Para obtener más información, consulte Cuotas de Amazon VPC en la Guía del usuario de Amazon VPC.

Cada política Network Firewall de Firewall Manager crea un firewall de Network Firewall con una política de firewall asociada y sus grupos de reglas. Estos recursos de Network Firewall están sujetos a las cuotas que figuran en cuotas de AWS Network Firewall de la Guía para desarrolladores de Network Firewall.

Cuotas flexibles

AWS Firewall Manager tiene cuotas predeterminadas en cuanto al número de entidades por región. Puede solicitar un aumento de dichas cuotas.

Todos los tipos de políticas

Recurso	Cuota predeterminada por región
Cuentas por organización en AWS Organizations	Varía. Una invitación enviada a una cuenta computa para esta cuota. La cuenta se devuelve si la cuenta

Recurso	Cuota predeterminada por región
	invitada rechaza la invitación, la cuenta de administración cancela la invitación o la invitación caduca.
Políticas de Firewall Manager por organización en AWS Organizations.	50. Las especific aciones de `Global` y `US East (N. Virginia) Region` se refieren a la misma región, por lo que este límite se aplica al total de las pólizas combinadas de ambas.
Unidades organizativas incluidas en el ámbito de aplicación de la política de Firewall Manager.	20
Cuentas incluidas en el ámbito de una política de Firewall Manager si incluye y excluye explícitamente cuentas individuales.	200
Cuentas incluidas en el ámbito de una política de Firewall Manager si no incluye o excluye explícitamente cuentas individuales.	2.500
Etiquetas que incluyen o excluyen los recursos por política de Firewall Manager.	8
Número de conjuntos de recursos por cuenta.	20
Número de recursos por conjunto de recursos.	100
Número de conjuntos de recursos por política de Firewall Manager.	5

AWS WAF políticas

Recurso	Cuota predeterminada por región
AWS WAF grupos de reglas por cuenta de administrador de Firewall Manager.	100
AWS WAF Grupos de reglas clásicas por cuenta de administrador de Firewall Manager.	10
Grupos de reglas por AWS WAF política.	50

Políticas de grupos de seguridad comunes

Recurso	Cuota predeterminada por región.
Grupos de seguridad principales por política.	3
Instancias de Amazon VPC dentro del ámbito de aplicación por política y cuenta, incluidas las VPC compartidas.	100

Políticas de grupos de seguridad de auditoría de contenido

Recurso	Cuota predeterminada por región
Audite los grupos de seguridad por política.	1
Aplicaciones por lista de aplicaciones.	50
Listas de aplicaciones administradas personalizadas para las reglas que permiten todo el tráfico.	1
Listas de aplicaciones administradas personalizadas según las reglas de la política.	1
Listas de aplicaciones administradas personalizadas por cuenta.	10

Recurso	Cuota predeterminada por región
Protocolos por lista de protocolos.	5
Listas de protocolos gestionados personalizadas para cualquier configuración de una política.	1
Listas de protocolos gestionados personalizadas por cuenta.	10

Políticas de ACL de red

Recurso	Cuota predeterminada por región
Número de reglas de entrada por política de ACL de red, utilizadas para la primera o la última regla. Por ejemplo, puede tener 5 primeras y 0 últimas reglas de entrada, o 2 primeras y 3 últimas, pero no puede tener 4 primeras y 2 últimas.	5
Número de reglas de salida por política de ACL de red, que se utilizan para la primera o la última regla. Por ejemplo, puede tener 5 primeras y 0 últimas reglas de salida, o 2 primeras y 3 últimas, pero no puede tener 4 primeras y 2 últimas.	5

Políticas de DNS Firewall

Recurso	Cuota predeterminada por región
Grupos de reglas de firewall de DNS según la política de firewall de DNS.	2

Cuotas invariables

No se AWS Firewall Manager pueden cambiar las siguientes cuotas por región relacionadas con:

Todos los tipos de políticas

Recurso	Cuota por región
El número máximo de administradores de Firewall Manager que puede tener en una AWS Organizations organización. Debe tener un administrador predeterminado y hasta nueve administradores adicionales de Firewall Manager.	10

AWS WAF políticas

Recurso	Cuota por región
Total de unidades de capacidad de ACL web (WCU) para los grupos de reglas de una política de AWS WAF .	5 000

AWS WAF Políticas clásicas

Recurso	Cuota por región
AWS WAF Grupos de reglas clásicos por política.	2:1 grupo de reglas creado por el cliente y 1 grupo de AWS Marketplace reglas.
AWS WAF Reglas clásicas por grupo de reglas AWS WAF clásicas de Firewall Manager.	10

Políticas de auditoría de contenido del grupo de seguridad

Recurso	Cuota por región
Listas de aplicaciones administradas por Firewall Manager para cualquier configuración de una política.	1
El Firewall Manager administra listas de protocolos para cualquier configuración de una política.	1

Políticas de Network Firewall

Recurso	Cuota por región
Número de VPC que se pueden corregir automáticamente para una sola política.	1 000
La cantidad de CIDR de IPV4 que puede proporcionar para una sola política.	50

Monitoreo AWS WAF y AWS Firewall ManagerAWS Shield Advanced

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el desempeño de sus servicios.

> **Note**
>
> Para obtener información sobre la supervisión de sus recursos de Shield Advanced y la identificación de posibles eventos de DDoS mediante Shield Advanced, consulte AWS Shield.

A medida que empiece a supervisar estos servicios, debe crear un plan de supervisión que incluya respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la supervisión?
- ¿Qué recursos va a supervisar?
- ¿Con qué frecuencia va a supervisar estos recursos?
- ¿Qué herramientas de monitoreo va a utilizar?
- ¿Quién se encargará de realizar las tareas de monitoreo?
- ¿Quién debería recibir una notificación cuando surjan problemas?

El siguiente paso consiste en establecer un punto de referencia del desempeño de normal en su entorno. Para ello se mide el desempeño en distintos momentos y bajo distintas condiciones de carga. A medida que supervisa AWS WAF, Firewall Manager, Shield Advanced y los servicios relacionados almacenan los datos históricos de supervisión para poder compararlos con los datos de rendimiento actuales, identificar los patrones de rendimiento normales y las anomalías de rendimiento y diseñar métodos para solucionar los problemas.

Por lo AWS WAF tanto, debe supervisar los siguientes elementos como mínimo para establecer una base de referencia:

- El número de solicitudes web permitidas
- El número de solicitudes web bloqueadas

Temas

Herramientas de monitoreo

AWS proporciona varias herramientas que puede utilizar para monitorear AWS WAF y AWS Shield Advanced. Puede configurar algunas de estas herramientas para que supervisen por usted, pero otras herramientas requieren intervención manual. Le recomendamos que automatice las tareas de supervisión en la medida de lo posible.

Herramientas de monitoreo automatizadas

Puede utilizar las siguientes herramientas de supervisión automatizadas para observar AWS WAF AWS Shield Advanced e informar cuando algo va mal:

- Paneles de información general sobre el tráfico de la ACL web: para acceder a los resúmenes del tráfico web que evalúa una ACL web, vaya a la página de la ACL web en la AWS WAF consola y abra la pestaña de información general del tráfico.

  Los paneles de información general del tráfico proporcionan resúmenes casi en tiempo real de CloudWatch las métricas de Amazon que AWS WAF recopila cuando evalúa el tráfico web de tu aplicación. Puede ver resúmenes de todo el tráfico web y del tráfico evaluado por los grupos de reglas de mitigación inteligente de amenazas.

  Para obtener más información, consulte Paneles de información general sobre el tráfico de ACL web o vaya a los paneles de la consola.
- Amazon CloudWatch Alarms: observe una sola métrica durante un período de tiempo que especifique y realice una o más acciones en función del valor de la métrica en relación con un umbral determinado durante varios períodos de tiempo. La acción es una notificación enviada a un tema de Amazon Simple Notification Service (Amazon SNS) o a una política de Amazon EC2 Auto Scaling. Las alarmas invocan acciones únicamente en caso de cambios de estado sostenidos. CloudWatch las alarmas no invocarán acciones simplemente porque se encuentren en un estado determinado; el estado debe haber cambiado y mantenido durante un número específico de períodos. Para obtener más información, consulte Supervisión del uso CloudWatch de CloudFront la actividad.

> **Note**
>
> CloudWatch las métricas y las alarmas no están habilitadas para AWS Firewall Manager.

No solo puede usarlo CloudWatch para monitorear AWS WAF y proteger las métricas de Shield Advanced como se describe enMonitorización con Amazon CloudWatch, sino que también debe usarlo CloudWatch para monitorear la actividad de sus recursos protegidos. Para más información, consulte los siguientes temas:

- Supervisión de CloudFront la actividad mediante CloudWatch la Guía para CloudFront desarrolladores de Amazon
- Registro y supervisión en Amazon API Gateway en la Guía para desarrolladores de API Gateway
- CloudWatch Métricas para el balanceador de carga de aplicaciones en la guía del usuario de Elastic Load Balancing
- Supervisión e inicio de sesión en la Guía para desarrolladores de AWS AppSync
- Registro y supervisión en Amazon Cognito en la Guía para desarrolladores de Amazon Cognito
- Ver los registros de App Runner transmitidos a CloudWatch Logs y ver las métricas del servicio de App Runner incluidas CloudWatch en la AWS App Runner guía para desarrolladores

- Amazon CloudWatch Logs: supervisa, almacena y accede a tus archivos de registro desde AWS CloudTrail u otras fuentes. Para obtener más información, consulta ¿Qué es Amazon CloudWatch Logs? .
- Amazon CloudWatch Events: automatice sus AWS servicios y responda automáticamente a los eventos del sistema. Los eventos de AWS los servicios se envían a CloudWatch Events prácticamente en tiempo real, y usted puede especificar las acciones automatizadas que se llevarán a cabo cuando un evento cumpla con una regla que usted haya escrito. Para obtener más información, consulta ¿Qué es Amazon CloudWatch Events?
- AWS CloudTrail Supervisión de registros: comparta archivos de registro entre cuentas, supervise los archivos de CloudTrail registro en tiempo real enviándolos a CloudWatch Logs, cree aplicaciones de procesamiento de registros en Java y valide que sus archivos de registro no hayan cambiado después de su entrega. CloudTrail Para obtener más información, consulte la sección Registro de llamadas a la API de AWS CloudTrail con Cómo trabajar con archivos de CloudTrail registro en la Guía del AWS CloudTrail usuario.

- AWS Config— Consulta la configuración de AWS los recursos de tu AWS cuenta, incluida la relación entre los recursos y la forma en que se configuraban en el pasado, de modo que puedas ver cómo cambian las configuraciones y las relaciones a lo largo del tiempo.

Herramientas de monitoreo manuales

Otra parte importante del monitoreo AWS WAF AWS Shield Advanced consiste en monitorear manualmente los elementos que las CloudWatch alarmas no cubren. Puede ver Shield Advanced y otros AWS Management Console paneles para ver el estado de su AWS entorno. AWS WAF CloudWatch Le recomendamos que también compruebe los archivos de registro de los ACL y reglas de su web.

- Por ejemplo, para ver el AWS WAF panel:
  - En la pestaña Solicitudes de la página ACL AWS WAF web, consulte un gráfico del total de solicitudes y solicitudes que coinciden con cada regla que haya creado. Para obtener más información, consulte Visualizar una muestra de solicitudes web.
- Consulte la página de CloudWatch inicio para ver lo siguiente:
  - Alarmas y estado actual
  - Gráficos de alarmas y recursos
  - Estado de los servicios

  Además, puede CloudWatch hacer lo siguiente:
  - Crear paneles personalizados para supervisar los servicios que le importan.
  - Realizar un gráfico con los datos de las métricas para resolver problemas y descubrir tendencias.
  - Busca y examina todas las métricas de tus AWS recursos.
  - Crear y editar las alarmas de notificación de problemas.

Monitorización con Amazon CloudWatch

Puedes monitorear las solicitudes web y las ACL y reglas web con Amazon CloudWatch, que recopila y procesa datos sin procesar a partir de métricas legibles AWS WAF y prácticamente en tiempo real para AWS Shield Advanced convertirlos en métricas legibles. Puedes usar las estadísticas de Amazon CloudWatch para obtener una perspectiva del rendimiento de tu aplicación

o servicio web. Para obtener más información, consulta Qué hay CloudWatch en la Guía del CloudWatch usuario de Amazon.

> **Note**
>
> CloudWatch las métricas y las alarmas no están habilitadas para Firewall Manager.

Puede crear una CloudWatch alarma de Amazon que envíe un mensaje de Amazon SNS cuando la alarma cambie de estado. Una alarma vigila una única métrica durante el periodo especificado y realiza una o varias acciones en función del valor de la métrica en relación con un determinado umbral durante una serie de periodos de tiempo. La acción es una notificación que se envía a un tema de Amazon SNS o a una política de escalado automático. Las alarmas invocan acciones únicamente en caso de cambios de estado sostenidos. CloudWatch las alarmas no invocan acciones simplemente porque se encuentran en un estado determinado; el estado debe haber cambiado y se ha mantenido durante un número específico de períodos.

Temas

Visualización de métricas y dimensiones

Las métricas se agrupan primero por el espacio de nombres del servicio y, después, por las distintas combinaciones de dimensiones de cada espacio de nombres. AWS Firewall Manager no registra las métricas.

- El AWS WAF espacio de nombres es `AWS/WAFV2`
- El espacio de nombres Shield Advanced es `AWS/DDoSProtection`

> **Note**
>
> AWS WAF informa las métricas una vez por minuto.

Shield Advanced informa de las métricas una vez por minuto durante un evento y con menos frecuencia otras veces.

Utilice los siguientes procedimientos para ver las métricas de AWS WAF y AWS Shield Advanced.

Para ver las métricas mediante la CloudWatch consola

1. Inicie sesión en la CloudWatch consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudwatch/.
2. Si es necesario, cambia la región por aquella en la que se encuentran tus AWS recursos. Para CloudFront, elija la región EE.UU. Este (Virginia del Norte).
3. En el panel de navegación, en Métricas, seleccione Todas las métricas y, a continuación, busca el servicio en la pestaña Explorar.

Para ver las métricas mediante la AWS CLI

- Para AWS/WAFV2, utilice el siguiente comando cuando se lo soliciten:

```
aws cloudwatch list-metrics --namespace "AWS/WAFV2"
```

  Para &SHDADV;, utilice el siguiente comando cuando se lo soliciten:

```
aws cloudwatch list-metrics --namespace "AWS/DDoSProtection"
```

AWS WAF métricas y dimensiones

AWS WAF informa las métricas una vez por minuto. AWS WAF proporciona métricas y dimensiones en el espacio de `AWS/WAFV2` nombres.

Puede ver la información resumida de las AWS WAF métricas a través de la AWS WAF consola, en la pestaña de resumen del tráfico de la ACL web. Para obtener más información, vaya a la consola o consulte Paneles de información general sobre el tráfico de ACL web.

Puede ver las siguientes métricas para las ACL web, las reglas, los grupos de reglas y las etiquetas.

- Tus reglas: las métricas se agrupan según la acción de la regla. Por ejemplo, cuando pruebas una regla en Count modo, sus coincidencias se muestran como `Count` métricas para la ACL web.
- Sus grupos de reglas: las métricas de sus grupos de reglas se muestran en las métricas del grupo de reglas.
- Grupos de reglas que pertenecen a otra cuenta: las métricas de los grupos de reglas, por lo general, solo las puede ver el propietario del grupo de reglas. Sin embargo, si anulas la acción de la regla para una regla, las métricas de esa regla aparecerán en las métricas de tu ACL web. Además, las etiquetas agregadas por cualquier grupo de reglas aparecen en las métricas de su ACL web

  Los grupos de reglas de esta categoría son AWS Reglas administradas para AWS WAF AWS Marketplace grupos de reglas gestionadosGrupos de reglas proporcionados por otros servicios, y los grupos de reglas que otra cuenta comparte contigo.
- Etiquetas: las etiquetas que se agregaron a una solicitud web durante la evaluación aparecen en las métricas de etiquetas de la ACL web. Puede acceder a las métricas de todas las etiquetas, independientemente de si las han agregado sus reglas y grupos de reglas o si las han agregado las reglas de un grupo de reglas propiedad de otra cuenta.

Temas

ACL web, grupo de reglas y métricas y dimensiones de reglas

ACL web, grupo de reglas y métricas de reglas

Métrica	Descripción
`AllowedRequests`	El número de solicitudes web permitidas. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma
`BlockedRequests`	El número de solicitudes web bloqueadas.

Métrica	Descripción
	Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma
`CountedRequests`	El número de solicitudes web contabilizadas. Criterios del informe: hay un valor distinto de cero. Una solicitud web contada es aquella que coincide con al menos una de las reglas. Normalmente se utiliza el conteo de solicitudes para las pruebas. Estadísticas válidas: suma
`CaptchaRequests`	El número de solicitudes web a las que se aplicaron controles de CAPTCHA. Criterios del informe: hay un valor distinto de cero. Una solicitud web de CAPTCHA es aquella que coincide con una regla que tiene una configuración de acción de CAPTCHA. Esta métrica registra todas las solicitudes que coinciden, independientemente de si tienen un token CAPTCHA válido. Estadísticas válidas: suma
`RequestsWithValidCaptchaToken`	El número de solicitudes web a las que se aplicaron controles de CAPTCHA y a las que se les aplicó un token de CAPTCHA válido. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma

Métrica	Descripción
`CaptchasAttempted`	El número de soluciones que presentó un usuario final en respuesta a un desafío relacionado con el sistema CAPTCHA. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma
`CaptchasSolved`	El número de soluciones de rompecabezas con CAPTCHA enviadas que resolvieron correctamente el rompecabezas. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma
`ChallengeRequests`	El número de solicitudes web a las que se aplicaron controles de impugnación. Criterios del informe: hay un valor distinto de cero. Una solicitud web de desafío es aquella que coincide con una regla que tiene una configuración de acción de Challenge. Esta métrica registra todas las solicitudes que coinciden, independientemente de si tienen un token de desafío válido. Estadísticas válidas: suma
`RequestsWithValidChallengeToken`	El número de solicitudes web a las que se aplicaron controles de impugnación y a las que se les aplicó un token de impugnación válido. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma

Métrica	Descripción
`PassedRequests`	El número de solicitudes aprobadas. Solo se usa para las solicitudes que se someten a una evaluación de un grupo de reglas sin coincidir con ninguna de las reglas del grupo de reglas. Criterios del informe: hay un valor distinto de cero. Las solicitudes transmitidas son solicitudes que no coinciden con ninguna de las reglas incluidas en el grupo de reglas. Estadísticas válidas: Suma

Dimensiones de ACL web, grupo de reglas y reglas

Dimensión	Descripción
`Region`	Necesario para todos los tipos de recursos protegidos, excepto para CloudFront las distribuciones de Amazon.
`Rule`	Uno de los siguientes: • El nombre de la métrica de la `Rule`. • ALL, que representa a todas las reglas de una WebACL o un `RuleGroup` . • `Default_Action` (solo cuando se combina con la dimensión de `WebACL`), que represent a la acción asignada a cualquier solicitud cuya evaluación no haya finalizado por la acción de una regla de la ACL web.
`RuleGroup`	El nombre de la métrica de la `RuleGroup` .
`WebACL`	El nombre de la métrica de la `WebACL`.

Dimensión	Descripción
`Country`	País de origen de la solicitud. Esta es la designación de dos caracteres de la norma 3166 de la Organización Internacional de Normalización (ISO). Por ejemplo, EE. UU. para Estados Unidos y UA para Ucrania. Si una solicitud tiene un encabezado de `X-Forwarded-For` , AWS WAF usa para determinar esta configuración. De lo contrario, AWS WAF utiliza el país de la IP del cliente. Esta determinación es independiente de la lógica que utilices en tus reglas para determinar el país de origen. AWS WAF determina las ubicaciones de las IP mediante bases de datos de MaxMind GeoIP.
`Attack`	El tipo de ataque AWS WAF identificado en la solicitud, en función de las reglas y los grupos de reglas que utilice en su ACL web. Sus reglas y las reglas de los grupos de reglas AWS gestionados básicos pueden identificar los tipos de ataques. Por ejemplo, las coincidencias de reglas de scripting entre sitios (XSS) identifican los tipos de ataques XSS y las reglas basadas en tasas identifican los tipos de ataques volumétricos. El tipo de ataque suele indicar el tipo de regla que puso fin a la evaluación de la solicitud web.
`Device`	El tipo de dispositivo del cliente que envió la solicitud , obtenido del encabezado de `user-agent` de la solicitud web.
`ManagedRuleGroup`	El nombre de la métrica de la `ManagedRuleGroup` .

Dimensión	Descripción
`ManagedRuleGroupRule`	La regla incluida en la `ManagedRuleGroup` que coincidió.

Etiquetar métricas y dimensiones

Métricas de las etiquetas agregadas a las solicitudes durante la evaluación por sus reglas y por los grupos de reglas administrados que usa en su ACL web. Para obtener más información, consulte Etiquetas en las solicitudes web.

Para cada solicitud web individual, AWS WAF almacena las métricas de un máximo de 100 etiquetas. Su evaluación de ACL web puede aplicar más de 100 etiquetas y compararlas con más de 100 etiquetas, pero solo las 100 primeras se reflejan en las métricas.

Métricas de etiquetas

Métrica	Descripción
`AllowedRequests`	El número de etiquetas en las solicitudes web a las que Allow aplicó la configuración de acción. Las etiquetas se pueden haber añadido en cualquier momento durante la evaluación de la solicitud web. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma
`BlockedRequests`	El número de etiquetas en las solicitudes web a las que Block aplicó la configuración de acción. Las etiquetas se pueden haber añadido en cualquier momento durante la evaluación de la solicitud web. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma
`CountedRequests`	El número de etiquetas agregadas a las solicitudes web por las reglas del grupo de reglas que tienen una configuración de acción de Count.

Métrica	Descripción
	Esta métrica solo está disponible para el propietario de un grupo de reglas, para las reglas incluidas en el grupo de reglas. En otros casos, las métricas de la etiqueta de recuento se agrupan en la acción de finalización que se aplicó a la solicitud, por ejemplo, Allow o Block. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma
`CaptchaRequests`	El número de etiquetas en las solicitudes web a las que se aplicó una acción de CAPTCHA terminal. Las etiquetas se pueden haber añadido en cualquier momento durante la evaluación de la solicitud web. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma
`ChallengeRequests`	El número de etiquetas en las solicitudes web a las que se aplicó una acción de Challenge terminal. Las etiquetas se pueden haber añadido en cualquier momento durante la evaluación de la solicitud web. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma
`AllowRuleMatch`	El número de reglas coincidentes que generaron la etiqueta asociada y finalizaron la evaluación de la solicitud con una Allow acción. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma

Métrica	Descripción
`BlockRuleMatch`	El número de reglas coincidentes que generaron la etiqueta asociada y finalizaron la evaluación de la solicitud con una Block acción. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma
`CountRuleMatch`	El número de reglas coincidentes que generaron la etiqueta asociada y aplicaron una Count acción. Una solicitud podría generar varias instancias de esta métrica si se configuran varias reglas con la misma etiqueta y acción. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma
`CaptchaRuleMatch`	El número de reglas coincidentes que generaron la etiqueta asociada y finalizaron la evaluación de la solicitud con una CAPTCHA acción. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma
`ChallengeRuleMatch`	El número de reglas coincidentes que generaron la etiqueta asociada y finalizaron la evaluación de la solicitud con una Challenge acción. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma

Métrica	Descripción
`CaptchaRuleMatchWithValidToken`	El número de reglas coincidentes que generaron la etiqueta asociada y aplicaron una acción permanente. CAPTCHA Una solicitud podría generar varias instancias de esta métrica si se configuran varias reglas con la misma etiqueta y acción. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma
`ChallengeRuleMatchWithValidToken`	El número de reglas coincidentes que generaron la etiqueta asociada y aplicaron una acción continua. Challenge Una solicitud podría generar varias instancias de esta métrica si se configuran varias reglas con la misma etiqueta y acción. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma

Dimensiones de etiquetas

Dimensión	Descripción
`Region`	Necesario para todos los tipos de recursos protegidos, excepto para CloudFront las distribuciones de Amazon.
`WebACL`	El nombre de la métrica de la `WebACL`.
`RuleGroup`	El nombre de la métrica de la `RuleGroup` . Utilizado para la métrica `CountedRequests` .

Dimensión	Descripción
`LabelNamespace`	El prefijo del espacio de nombres de la etiqueta que se agregó a la solicitud.
`Label`	El nombre de la etiqueta que se agregó a la solicitud.
`Context`	El grupo de reglas gestionado que sirvió de contexto para la adición de la etiqueta. Por ejemplo, el contexto de las etiquetas de administración de tokens `awswaf:managed:token:accepted` es el grupo de reglas AWS WAF gestionadas que utiliza la gestión de fichas en la solicitud, como el grupo de reglas gestionado por Bot Control o ATP. Esta dimensión no se aplica a todas las etiquetas.

Métricas y dimensiones de visibilidad de bots gratuitas

Si no utilizas Bot Control en tu ACL web, AWS WAF aplica el grupo de reglas gestionado por Bot Control a una muestra de tus solicitudes web, sin coste adicional. Esto puede darte una idea del tráfico de bots que llega a sus recursos protegidos. Para obtener información sobre el control de bots, consulte AWS WAF Grupo de reglas de control de bots.

Métricas de visibilidad de bots gratuitas

Métrica	Descripción
`SampleAllowedRequest`	El número de solicitudes muestreadas que tienen Allow acción. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma
`SampleBlockedRequest`	El número de solicitudes muestreadas que requieren una Block acción. Criterios del informe: hay un valor distinto de cero.

Métrica	Descripción
	Estadísticas válidas: suma
`SampleCaptchaRequest`	El número de solicitudes muestreadas que requieren una CAPTCHA acción. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma
`SampleChallengeRequest`	El número de solicitudes muestreadas que requieren una Challenge acción. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma
`SampleCountRequest`	El número de solicitudes muestreadas que requieren una Count acción. Criterios del informe: hay un valor distinto de cero. Estadísticas válidas: suma

Dimensiones de visibilidad de los bots gratuitas

Dimensión	Descripción
`Region`	Necesario para todos los tipos de recursos protegidos, excepto para CloudFront las distribuciones de Amazon.
`WebACL`	El nombre de la métrica de la `WebACL`.
`BotCategory`	El nombre de la categoría de bots detectada, según las etiquetas de las solicitudes web.
`VerificationStatus`	El nombre del estado de verificación del bot detectado, basado en las etiquetas de solicitud web.

Dimensión	Descripción
`Signal`	El nombre de las señales de bot detectadas, según las etiquetas de solicitud web.

AWS Shield Advanced métricas

Shield Advanced publica las métricas de CloudWatch detección, mitigación y principales contribuyentes de Amazon para todos los recursos que protege. Estas métricas mejoran su capacidad de supervisar sus recursos, ya que permiten crear y configurar CloudWatch paneles y alarmas para ellos.

La consola Shield Advanced presenta resúmenes de muchas de las métricas que registra. Para obtener más información, consulte Visibilidad de los eventos de DDoS.

Si habilita la mitigación automática de DDoS en la capa de aplicación para la protección de la capa de aplicaciones,

Ubicaciones de informes métricos

Shield Advanced obtiene información sobre métricas de la región del Este de EE. UU. (Norte de Virginia), `us-east-1` para:

- Los servicios globales Amazon CloudFront y Amazon Route 53.
- Grupos de protección. Para obtener más información sobre la protección degrupos, consulte AWS Shield Advanced grupos de protección.

Para otros tipos de recursos, Shield Advanced informa de las métricas de la región del recurso.

Plazo de presentación de informes métricos

Shield Advanced informa a Amazon de las métricas CloudWatch de un AWS recurso con más frecuencia durante los eventos de DDoS que cuando no hay ningún evento en curso. Shield Advanced informa de las métricas una vez por minuto durante un evento y, después, una vez finalizado el evento.

Aunque no haya eventos en curso, Shield Advanced notifica las métricas una vez al día, a una hora asignada al recurso. Este informe periódico mantiene las métricas activas y disponibles para su uso en CloudWatch alarmas y paneles personalizados.

Recomendaciones de alarmas

Le recomendamos que cree alarmas para notificarle las circunstancias que requieren atención. Como punto de partida, puede crear una alarma para cada recurso protegido que informe cuando la métrica `DDoSDetected` de detección no sea cero. Un valor distinto de cero en esta métrica no implica necesariamente que se esté produciendo un ataque DDoS, pero recomendamos analizar más detenidamente el estado del recurso cuando la métrica se encuentre en este estado.

En el caso de una avalancha de solicitudes, le recomendamos que cree alarmas para realizar comprobaciones compuestas que también tengan en cuenta factores como el estado de las aplicaciones y el volumen de solicitudes web. Puede optar por utilizar la alarma en las otras tres métricas que informan sobre el volumen de tráfico para diversas dimensiones del vector de ataque. Al tener en cuenta la capacidad de su aplicación y las alarmas cuando el tráfico se acerca a las limitaciones de la aplicación, se puede crear un conjunto de reglas que notifiquen cuando sea necesario, sin generar demasiados ruidos no deseados.

Temas

Métricas de detección

Shield Advanced proporciona las métricas y dimensiones del espacio de `AWS/DDoSProtection` nombres.

Métricas de detección

Métrica	Descripción
`DDoSDetected`	Indica si se está realizando un evento DDoS para un nombre de recurso de Amazon (ARN) determinado. Esta métrica tiene un valor distinto de cero durante un evento.
`DDoSAttackBitsPerSecond`	El número de bits observados durante un evento DDoS para un nombre de recurso de

Métrica	Descripción
	Amazon (ARN) determinado. Esta métrica está disponible solo para eventos DDoS de capa de red y transporte (capa 3 y capa 4). Esta métrica tiene un valor distinto de cero durante un evento. Unidades: bits
`DDoSAttackPacketsPerSecond`	El número de paquetes observados durante un evento DDoS para un nombre de recurso de Amazon (ARN) determinado. Esta métrica está disponible solo para eventos DDoS de capa de red y transporte (capa 3 y capa 4). Esta métrica tiene un valor distinto de cero durante un evento. Unidades: paquetes
`DDoSAttackRequestsPerSecond`	El número de solicitudes observadas durante un evento DDoS para un nombre de recurso de Amazon (ARN) determinado. Esta métrica está disponible solo para los eventos DDoS de la capa 7. Esta métrica se registra solo para los eventos de la capa 7 más importantes. Esta métrica tiene un valor distinto de cero durante un evento. Unidades: solicitudes

Shield Advanced publica la métrica de `DDoSDetected` sin otras dimensiones. Las métricas de detección restantes incluyen las dimensiones de `AttackVector` que corresponden al tipo de ataque, de la siguiente lista:

- `ACKFlood`

- ChargenReflection
- DNSReflection
- GenericUDPReflection
- MemcachedReflection
- MSSQLReflection
- NetBIOSReflection
- NTPReflection
- PortMapper
- RequestFlood
- RIPReflection
- SNMPReflection
- SSDPReflection
- SYNFlood
- UDPFragment
- UDPTraffic
- UDPReflection

Métricas de mitigación

Shield Advanced proporciona métricas y dimensiones en el espacio de AWS/DDoSProtection nombres.

Métricas de mitigación

Métrica	Descripción
VolumePacketsPerSecond	La cantidad de paquetes por segundo que una mitigación implementada en respuesta a un evento detectado descartó o aprobó. Unidades: paquetes

Dimensiones de mitigación

Dimensión	Descripción
`ResourceArn`	Nombre de recurso de Amazon (ARN)
`MitigationAction`	El resultado de una mitigación aplicada. Los valores posibles son `Pass` o `Drop`.

Métricas de los principales colaboradores

Shield Advanced proporciona métricas en el espacio de `AWS/DDoSProtection` nombres.

Métricas de los principales colaboradores

Métrica	Descripción
`VolumePacketsPerSecond`	El número de paquetes por segundo para un colaborador principal. Unidades: paquetes
`VolumeBitsPerSecond`	El número de bits por segundo de un contribuy ente principal. Unidades: bits

Shield Advanced publica las métricas de los principales colaboradores por combinaciones de dimensiones que caracterizan a los colaboradores del evento. Puede utilizar cualquiera de las siguientes combinaciones de dimensiones para cualquiera de las métricas de principales contribuyentes:

- `ResourceArn`, `Protocol`
- `ResourceArn`, `Protocol`, `SourcePort`
- `ResourceArn`, `Protocol`, `DestinationPort`
- `ResourceArn`, `Protocol`, `SourceIp`
- `ResourceArn`, `Protocol`, `SourceAsn`
- `ResourceArn`, `TcpFlags`

Dimensiones de principales contribuyentes

Dimensión	Descripción
`ResourceArn`	Nombre de recurso de Amazon (ARN).
`Protocol`	Nombre del protocolo IP, ya sea `TCP` o `UDP`.
`SourcePort`	Puerto TCP o UDP de origen.
`DestinationPort`	Puerto TCP o UDP de destino.
`SourceIp`	Dirección IP de origen.
`SourceAsn`	Número de sistema autónomo (ASN) de origen.
`TcpFlags`	Combinación de indicadores presentes en un paquete TCP, separados por un guión (`-`). Los indicadores monitoreados son `ACK`, `FIN`, `RST`, `SYN`. Este valor de dimensión siempre aparece ordenado alfabéticamente. Por ejemplo, `ACK-FIN-RST-SYN` , `ACK-SYN` y `FIN-RST`.

AWS Firewall Manager notificaciones

AWS Firewall Manager no registra las métricas, por lo que no puede crear CloudWatch alarmas de Amazon específicamente para Firewall Manager. Sin embargo, puede configurar notificaciones de Amazon SNS para que le avisen ante posibles ataques. Para crear notificaciones de Amazon SNS en Firewall Manager, consulte Paso 4: Configurar las notificaciones de Amazon SNS y las alarmas de Amazon CloudWatch .

Registro de llamadas a la API de AWS CloudTrail con

AWS WAF AWS Shield Advanced, y AWS Firewall Manager están integrados con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio. CloudTrail captura un subconjunto de llamadas a la API para estos servicios como eventos, incluidas las llamadas desde las AWS WAF consolas Shield Advanced o Firewall Manager y desde las llamadas en código a las AWS WAF API Shield Advanced o Firewall Manager. Si crea una ruta,

puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de AWS WAF Shield Advanced o Firewall Manager. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada CloudTrail, puede determinar la solicitud que se realizó a estos servicios, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, incluido cómo configurarlo y habilitarlo, consulte la Guía del AWS CloudTrail usuario.

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad de eventos admitida en AWS WAF Shield Advanced o Firewall Manager, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de los eventos en su Cuenta de AWS cuenta, incluidos los AWS WAF eventos de Shield Advanced o Firewall Manager, cree un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, este se aplica a todas las regiones. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail Integraciones y servicios compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

AWS WAF información en AWS CloudTrail

Todas AWS WAF las acciones se registran AWS CloudTrail y se documentan en la Referencia de la AWS WAF API. Por ejemplo, las llamadas a los `ListWebACL` archivos de CloudTrail registro y las `DeleteWebACL` generan entradas en ellos. `UpdateWebACL`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz
- si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado
- Si la solicitud la realizó otro AWS servicio

Para obtener más información, consulte CloudTrailUserIdentity Element.

Ejemplo: AWS WAF entradas de un archivo de registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. AWS CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud específica realizada desde un origen cualquiera, y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro de pila ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

Los siguientes son ejemplos de entradas de CloudTrail registro para las operaciones de ACL AWS WAF web.

Ejemplo: entrada de CloudTrail registro para `CreateWebACL`


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T03:43:07Z"
```

```
      }
    }
  },
  "eventTime": "2019-11-06T03:44:21Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "CreateWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "defaultAction": {
      "block": {}
    },
    "description": "foo",
    "rules": [
      {
        "name": "foo",
        "priority": 1,
        "statement": {
          "geoMatchStatement": {
            "countryCodes": [
              "AF",
              "AF"
            ]
          }
        },
        "action": {
          "block": {}
        },
        "visibilityConfig": {
          "sampledRequestsEnabled": true,
          "cloudWatchMetricsEnabled": true,
          "metricName": "foo"
        }
      }
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    }
```

```
  },
  "responseElements": {
    "summary": {
      "name": "foo",
      "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
      "description": "foo",
      "lockToken": "67551e73-49d8-4363-be48-244deea72ea9",
      "aRN": "arn:aws:wafv2:us-east-1:112233445566:global/webacl/foo/
ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b"
    }
  },
  "requestID": "c51521ba-3911-45ca-ba77-43aba50471ca",
  "eventID": "afd1a60a-7d84-417f-bc9c-7116cf029065",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

Ejemplo: entrada de CloudTrail registro para `GetWebACL`

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AssumedRole",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AssumedRole",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
```

```
  "eventTime": "2019-11-06T19:18:28Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "GetWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "webacl"
  },
  "responseElements": null,
  "requestID": "f2db4884-4eeb-490c-afe7-67cbb494ce3b",
  "eventID": "7d563cd6-4123-4082-8880-c2d1fda4d90b",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

Ejemplo: entrada de CloudTrail registro para `UpdateWebACL`

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
```

```
      }
    }
  },
  "eventTime": "2019-11-06T19:20:56Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "UpdateWebACL",
  "awsRegion": ""us-east-1,
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "defaultAction": {
      "block": {}
    },
    "description": "foo",
    "rules": [
      {
        "name": "foo",
        "priority": 1,
        "statement": {
          "geoMatchStatement": {
            "countryCodes": [
              "AF"
            ]
          }
        },
        "action": {
          "block": {}
        },
        "visibilityConfig": {
          "sampledRequestsEnabled": true,
          "cloudWatchMetricsEnabled": true,
          "metricName": "foo"
        }
      }
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    },
```

```
    "lockToken": "67551e73-49d8-4363-be48-244deea72ea9"
  },
  "responseElements": {
    "nextLockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "requestID": "41c96e12-9790-46ab-b145-a230f358f2c2",
  "eventID": "517a10e6-4ca9-4828-af90-a5cff9756594",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

Ejemplo: entrada de CloudTrail registro para `DeleteWebACL`

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/session-name",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:25:17Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "DeleteWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
```

```
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "lockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "responseElements": null,
  "requestID": "71703f89-e139-440c-96d4-9c77f4cd7565",
  "eventID": "2f976624-b6a5-4a09-a8d0-aa3e9f4e5187",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

Ejemplo: entradas de un archivo de registro AWS WAF clásico

AWS WAF Classic es la versión anterior de AWS WAF. Para obtener más información, consulte AWS WAF Clásico.

La entrada de registro muestra las operaciones `CreateRule`, `GetRule`, `UpdateRule` y `DeleteRule`:

```
{
  "Records": [
   {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:14Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "CreateRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
```

```
        "name": "0923ab32-7229-49f0-a0e3-66c81example",
        "changeToken": "l9434322-8685-4ed2-9c5b-9410bexample",
        "metricName": "0923ab32722949f0a0e366c81example"
      },
      "responseElements": {
        "rule": {
          "metricName": "0923ab32722949f0a0e366c81example",
          "ruleId": "12132e64-6750-4725-b714-e7544example",
          "predicates": [

          ],
          "name": "0923ab32-7229-49f0-a0e3-66c81example"
        },
        "changeToken": "l9434322-8685-4ed2-9c5b-9410bexample"
      },
      "requestID": "4e6b66f9-d548-11e3-a8a9-73e33example",
      "eventID": "923f4321-d378-4619-9b72-4605bexample",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:22Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "GetRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "ruleId": "723c2943-82dc-4bc1-a29b-c7d73example"
      },
      "responseElements": null,
      "requestID": "8e4f3211-d548-11e3-a8a9-73e33example",
      "eventID": "an236542-d1f9-4639-bb3d-8d2bbexample",
      "eventType": "AwsApiCall",
```

```
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:13Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "UpdateRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "ruleId": "7237b123-7903-4d9e-8176-9d71dexample",
        "changeToken": "32343a11-35e2-4dab-81d8-6d408example",
        "updates": [
          {
            "predicate": {
              "type": "SizeConstraint",
              "dataId": "9239c032-bbbe-4b80-909b-782c0example",
              "negated": false
            },
            "action": "INSERT"
          }
        ]
      },
      "responseElements": {
        "changeToken": "32343a11-35e2-4dab-81d8-6d408example"
      },
      "requestID": "11918283-0b2d-11e6-9ccc-f9921example",
      "eventID": "00032abc-5bce-4237-a8ee-5f1a9example",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
```

```
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:28Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "DeleteRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "changeToken": "fd232003-62de-4ea3-853d-52932example",
        "ruleId": "3e3e2d11-fd8b-4333-8b03-1da95example"
      },
      "responseElements": {
        "changeToken": "fd232003-62de-4ea3-853d-52932example"
      },
      "requestID": "b23458a1-0b2d-11e6-9ccc-f9928example",
      "eventID": "a3236565-1a1a-4475-978e-81c12example",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    }
  ]
}
```


AWS Shield Advanced información en CloudTrail

AWS Shield Advanced admite el registro de las siguientes acciones como eventos en los archivos de CloudTrail registro:

- ListAttacks
- DescribeAttack
- CreateProtection
- DescribeProtection
- DeleteProtection
- ListProtections

- CreateSubscription
- DescribeSubscription
- GetSubscriptionState

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento CloudTrail UserIdentity.

Ejemplo: entradas de archivos de registro de Shield Advanced

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que muestra las `ListProtections` acciones `DeleteProtection` y.


```
[
 {
   "eventVersion": "1.05",
   "userIdentity": {
     "type": "IAMUser",
     "principalId": "123456789098765432123 1",
     "arn": "arn:aws:iam::123456789012:user/SampleUser",
     "accountId": "123456789012",
     "accessKeyId": "1AFGDT647FHU83JHFI81H",
     "userName": "SampleUser"
   },
```

```
    "eventTime": "2018-01-10T21:31:14Z",
    "eventSource": "shield.amazonaws.com",
    "eventName": "DeleteProtection",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
    "requestParameters": {
      "protectionId": "12345678-5104-46eb-bd03-agh4j8rh3b6n"
    },
    "responseElements": null,
    "requestID": "95bc0042-f64d-11e7-abd1-1babdc7aa857",
    "eventID": "85263bf4-17h4-43bb-b405-fh84jhd8urhg",
    "eventType": "AwsApiCall",
    "apiVersion": "AWSShield_20160616",
    "recipientAccountId": "123456789012"
  },
  {
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "123456789098765432123",
      "arn": "arn:aws:iam::123456789012:user/SampleUser",
      "accountId": "123456789012",
      "accessKeyId": "1AFGDT647FHU83JHFI81H",
      "userName": "SampleUser"
    },
    "eventTime": "2018-01-10T21:30:03Z",
    "eventSource": "shield.amazonaws.com",
    "eventName": "ListProtections",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "6accca40-f64d-11e7-abd1-1bjfi8urhj47",
    "eventID": "ac0570bd-8dbc-41ac-a2c2-987j90j3h78f",
    "eventType": "AwsApiCall",
    "apiVersion": "AWSShield_20160616",
    "recipientAccountId": "123456789012"
  }
]
```

AWS Firewall Manager información en CloudTrail

AWS Firewall Manager admite el registro de las siguientes acciones como eventos en los archivos de CloudTrail registro:

- AssociateAdminAccount
- DeleteNotificationChannel
- DeletePolicy
- DisassociateAdminAccount
- PutNotificationChannel
- PutPolicy
- GetAdminAccount
- GetComplianceDetail
- GetNotificationChannel
- GetPolicy
- ListComplianceStatus
- ListPolicies

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento CloudTrail UserIdentity.

Ejemplo: Entradas de archivos de registro de Firewall Manager

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud,

etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que muestra la acción `GetAdminAccount` -->.


```
 {
                "eventVersion": "1.05",
                "userIdentity": {
                                "type": "AssumedRole",
                                "principalId": "123456789098765432123 1",
                                "arn": "arn:aws:sts::123456789012:assumed-role/Admin/
SampleUser",
                                "accountId": "123456789012",
                                "accessKeyId": "1AFGDT647FHU83JHFI81H",
                                "sessionContext": {
                                                "attributes": {
                                                                "mfaAuthenticated":
 "false",
                                                                "creationDate":
 "2018-04-14T02:51:50Z"
                                                },
                                                "sessionIssuer": {
                                                                "type": "Role",
                                                                "principalId":
 "123456789098765432123 1",
                                                                "arn":
 "arn:aws:iam::123456789012:role/Admin",
                                                                "accountId":
 "123456789012",
                                                                "userName": "Admin"
                                                 }
                                  }
                                },
                "eventTime": "2018-04-14T03:12:35Z",
                "eventSource": "fms.amazonaws.com",
                "eventName": "GetAdminAccount",
                "awsRegion": "us-east-1",
                "sourceIPAddress": "72.21.198.65",
                "userAgent": "console.amazonaws.com",
                "requestParameters": null,
                "responseElements": null,
```

```
            "requestID": "ae244f41-3f91-11e8-787b-dfaafef95fc1",
            "eventID": "5769af1e-14b1-4bd1-ba75-f023981d0a4a",
            "eventType": "AwsApiCall",
            "apiVersion": "2018-01-01",
            "recipientAccountId": "123456789012"
    }
```

Uso de la AWS Shield Advanced API AWS WAF and

En esta sección se describe cómo realizar solicitudes a la API de AWS WAF and Shield Advanced para crear y gestionar conjuntos de partidos, reglas y ACL web, así AWS WAF como tu suscripción y protecciones en Shield Advanced. En esta sección se darán a conocer los componentes de las solicitudes, el contenido de las respuestas y cómo autenticar solicitudes.

Temas

Uso de los AWS SDK

Si utilizas un lenguaje que AWS proporciona un SDK, úsalo en lugar de intentar abrirte paso a través de las API. Los SDK simplifican la autenticación, se integran fácilmente con su entorno de desarrollo y proporcionan un fácil acceso a los AWS WAF comandos Shield Advanced. Para obtener más información sobre los AWS SDK, consulte Descargar herramientas el tema. Configuración de su cuenta para usar los servicios

Realizar solicitudes HTTPS a AWS WAF o Shield Advanced

AWS WAF y las solicitudes Shield Advanced son solicitudes HTTPS, tal y como se define en el RFC 2616. Como cualquier solicitud HTTP, una solicitud a AWS WAF o Shield Advanced contiene un método de solicitud, un URI, encabezados de solicitud y un cuerpo de solicitud. La respuesta contiene un código de estado HTTP, encabezados de respuesta y, a veces, una respuesta.

URI de solicitud

La solicitud URI siempre es un signo de barra diagonal sencilla, `/`.

Encabezados HTTP

AWS WAF y Shield Advanced requieren la siguiente información en el encabezado de una solicitud HTTP:

Host (requerida)

Punto de conexión que especifica dónde se crean los recursos. Para obtener más información acerca de los puntos de enlace, consulte Puntos de enlace de servicio de AWS. Por ejemplo, el valor del `Host` encabezado AWS WAF de una CloudFront distribución es `waf.amazonaws.com:443`.

x-amz-date o Fecha (obligatorio)

Fecha utilizada para crear la firma que se encuentra en el encabezado de la `Authorization`. Especifique la fecha en formato estándar ISO 8601, hora UTC, tal y como se muestra en el ejemplo siguiente:

```
x-amz-date: 20151007T174952Z
```

Debe incluir `x-amz-date` o `Date`. (Algunas bibliotecas de cliente de HTTP no permiten configurar el encabezado de la `Date`). Cuando hay un `x-amz-date` encabezado, AWS WAF ignora cualquier `Date` encabezado al autenticar la solicitud.

La marca de tiempo debe estar a menos de 15 minutos de la hora del AWS sistema en que se recibe la solicitud. En caso contrario, la solicitud falla y emite el código de error `RequestExpired` para impedir que otra persona reproduzca sus solicitudes.

Authorization (requerida)

Información necesaria para solicitar la autenticación. Para obtener más información sobre la creación de este encabezado, consulte Autenticación de solicitudes.

X-Amz-Target (requerida)

Concatenación de `AWSWAF_` o `AWSShield_`, la versión de la API sin puntuación, un punto (`.`) y el nombre de la operación, por ejemplo:

`AWSWAF_20150824.CreateWebACL`

Content-Type (condicional)

Especifica que el tipo de contenido es JSON, así como la versión de JSON, tal y como se muestra en el ejemplo siguiente:

```
Content-Type: application/x-amz-json-1.1
```

Condición: obligatorio para las solicitudes de `POST`.

Content-Length (condicional)

Longitud del mensaje (sin encabezados) de acuerdo con RFC 2616.

Condición: obligatoria si el texto de la solicitud contiene información (la mayoría de los kits de herramientas agregan este encabezado automáticamente).

A continuación se muestra un ejemplo de un encabezado en una solicitud de HTTP para crear una ACL web en AWS WAF:

```
POST / HTTP/1.1
Host: waf.amazonaws.com:443
X-Amz-Date: 20151007T174952Z
Authorization: AWS4-HMAC-SHA256
               Credential=AccessKeyID/20151007/us-east-2/waf/aws4_request,
               SignedHeaders=host;x-amz-date;x-amz-target,

 Signature=145b1567ab3c50d929412f28f52c45dbf1e63ec5c66023d232a539a4afd11fd9
X-Amz-Target: AWSWAF_20150824.CreateWebACL
Accept: */*
Content-Type: application/x-amz-json-1.1; charset=UTF-8
Content-Length: 231
Connection: Keep-Alive
```

Cuerpo de la solicitud HTTP

Muchas acciones AWS WAF de la API Shield Advanced requieren que incluyas datos con formato JSON en el cuerpo de la solicitud.

La siguiente solicitud de ejemplo utiliza una declaración JSON simple para actualizar una `IPSet` e incluir la dirección IP 192.0.2.44 (representada en notación CIDR como 192.0.2.44/32):

```
POST / HTTP/1.1
Host: waf.amazonaws.com:443
X-Amz-Date: 20151007T174952Z
Authorization: AWS4-HMAC-SHA256
               Credential=AccessKeyID/20151007/us-east-2/waf/aws4_request,
               SignedHeaders=host;x-amz-date;x-amz-target,

 Signature=145b1567ab3c50d929412f28f52c45dbf1e63ec5c66023d232a539a4afd11fd9
```

```
X-Amz-Target: AWSWAF_20150824.UpdateIPSet
Accept: */*
Content-Type: application/x-amz-json-1.1; charset=UTF-8
Content-Length: 283
Connection: Keep-Alive

{
   "ChangeToken": "d4c4f53b-9c7e-47ce-9140-0ee5ffffffff",
   "IPSetId": "69d4d072-170c-463d-ab82-0643ffffffff",
   "Updates": [
      {
         "Action": "INSERT",
         "IPSetDescriptor": {
            "Type": "IPV4",
            "Value": "192.0.2.44/32"
         }
      }
   ]
}
```

Respuestas HTTP

Todas las acciones de la API AWS WAF y Shield Advanced incluyen datos con formato JSON en la respuesta.

Estos son algunos encabezados importantes en la respuesta HTTP y cómo debe controlarlos en su aplicación, si procede:

HTTP/1.1

Este encabezado viene seguido de un código de estado. El código de estado 200 indica el éxito de la operación.

Tipo: cadena

x-amzn- RequestId

Un valor creado por AWS WAF o Shield Advanced que identifica de forma exclusiva su solicitud, por ejemplo,`K2QH8DN0U907N97FNA2GDLL80BVV4KQNSO5AEMVJF66Q9ASUAAJG`. Si tiene algún problema con AWS WAF, AWS puede usar este valor para solucionar el problema.

Tipo: cadena

Content-Length

Longitud del cuerpo de la respuesta en bytes.

Tipo: cadena

Date

La fecha y la hora en que AWS WAF Shield Advanced respondió, por ejemplo, miércoles 7 de octubre de 2015 a las 12:00:00 GMT.

Tipo: String

Respuestas de error

Si una solicitud provoca un error, la respuesta HTTP contiene los siguientes valores:

- Un documento de error JSON como cuerpo de la respuesta
- Contenido-Tipo
- Código de estado HTTP de 3xx, 4xx o 5xx

A continuación se muestra un ejemplo de un documento de error JSON:

```
HTTP/1.1 400 Bad Request
x-amzn-RequestId: b0e91dc8-3807-11e2-83c6-5912bf8ad066
x-amzn-ErrorType: ValidationException
Content-Type: application/json
Content-Length: 125
Date: Mon, 26 Nov 2012 20:27:25 GMT

{"message":"1 validation error detected: Value null at 'TargetString' failed to satisfy
 constraint: Member must not be null"}
```

Autenticación de solicitudes

Si utilizas un lenguaje que AWS proporciona un SDK para, te recomendamos que utilices el SDK. Todos los AWS SDK simplifican enormemente el proceso de firma de solicitudes y te ahorran una cantidad de tiempo significativa en comparación con el uso de la API AWS WAF o Shield Advanced. Además, los SDK se integran fácilmente con su entorno de desarrollo y proporcionan acceso sencillo a los comandos relacionados.

AWS WAF y Shield Advanced requieren que autentiques todas las solicitudes que envíes firmando la solicitud. Para firmar una solicitud, se calcula una firma digital mediante una función hash criptográfica que proporciona un valor hash basado en la entrada. La entrada incluye el texto de la solicitud y su clave de acceso secreta. La función hash devuelve un valor hash que se incluye en la solicitud como la firma. La firma forma parte del encabezado de la `Authorization` de la solicitud.

Tras recibir su solicitud, AWS WAF Shield Advanced recalcula la firma mediante la misma función hash y la misma entrada que utilizó para firmar la solicitud. Si la firma resultante coincide con la firma de la solicitud, AWS WAF o Shield Advanced procesa la solicitud. De lo contrario, la solicitud es rechazada.

AWS WAF y Shield Advanced admite la autenticación mediante la versión 4 de AWS Signature. El proceso para calcular una firma se puede dividir en tres tareas:

Tarea 1: Creación de una solicitud canónica

Crear su solicitud HTTP en formato canónico como se describe en Tarea 1: Creación de una solicitud canónica para Signature Version 4 en Referencia general de Amazon Web Services.

Tarea 2: Creación de una cadena para firmar

Crear una cadena que se utilizará como uno de los valores de entrada de la función hash criptográfica. La cadena, llamada cadena para firmar, es una concatenación de los valores siguientes:

- Nombre del algoritmo de hash
- Fecha de solicitud
- Cadena en el ámbito de credenciales
- Solicitud estandarizada (canónica) desde la tarea anterior

La cadena del ámbito de credenciales es una concatenación de fecha, región e información del servicio.

Para el parámetro `X-Amz-Credential`, especifique lo siguiente:

- Código para el punto de conexión al que está enviando la solicitud, `us-east-2`
- `waf` para la abreviatura de servicio

Por ejemplo:

```
X-Amz-Credential=AKIAIOSFODNN7EXAMPLE/20130501/us-east-2/waf/
aws4_request
```

Tarea 3: Crear una firma

Crear una firma para su solicitud mediante una función hash criptográfica que acepta dos cadenas de entrada:

- La cadena para firmar, desde la Tarea 2.
- Una clave derivada. La clave derivada se calcula a partir de la clave de acceso secreta, utilizando el ámbito de credencial para crear una serie de códigos de autenticación de mensajes basados en hash (HMAC).

Información relacionada

Los recursos relacionados siguientes pueden serle de ayuda cuando trabaje con este servicio.

Los siguientes recursos están disponibles para AWS WAF AWS Shield Advanced, y AWS Firewall Manager.

- Directrices de implementación AWS WAF: publicación técnica con recomendaciones actuales de implementación AWS WAF para proteger las aplicaciones web nuevas y existentes.
- AWS foros de debate: un foro comunitario para debatir cuestiones técnicas relacionadas con este y otros AWS servicios.
- AWS WAF Foro de debate: un foro comunitario para que los desarrolladores discutan cuestiones técnicas relacionadas con. AWS WAF
- Foro de debate sobre Shield Advanced: un foro de la comunidad en el que los desarrolladores pueden debatir aspectos técnicos relacionados con Shield Advanced.
- AWS WAF información del producto: la página web principal con información sobre las características AWS WAF, los precios y mucho más.
- Información de producto de Shield Advanced: página web principal para obtener información sobre Shield Advanced, incluidos precios, características, etc.

Los siguientes recursos están disponibles para Amazon Web Services.

- Clases y talleres: enlaces a cursos especializados y basados en roles, además de laboratorios personalizados que te ayudarán a perfeccionar tus AWS habilidades y a adquirir experiencia práctica.
- AWS Centro para desarrolladores: explore los tutoriales, descargue herramientas y obtenga información sobre los eventos para desarrolladores. AWS
- AWS Herramientas para desarrolladores: enlaces a herramientas para desarrolladores, SDK, kits de herramientas IDE y herramientas de línea de comandos para desarrollar y administrar AWS aplicaciones.
- Centro de recursos de introducción: aprenda a configurar su primera aplicación Cuenta de AWS, a unirse a la AWS comunidad y a lanzar su primera aplicación.
- Tutoriales prácticos: sigue step-by-step los tutoriales para lanzar tu primera aplicación. AWS

- AWS Documentos técnicos: enlaces a una lista completa de AWS documentos técnicos, que abarcan temas como la arquitectura, la seguridad y la economía, redactados por arquitectos de AWS soluciones u otros expertos técnicos.
- AWS Support Center: el centro para crear y gestionar sus casos. AWS Support También incluye enlaces a otros recursos útiles, como foros, preguntas frecuentes técnicas, estado del servicio y AWS Trusted Advisor.
- AWS Support— La página web principal con información sobre AWS Support un one-on-one canal de soporte de respuesta rápida que le ayudará a crear y ejecutar aplicaciones en la nube.
- Contacte con nosotros – Un punto central de contacto para las consultas relacionadas con la facturación AWS , cuentas, eventos, abuso y demás problemas.
- AWS Condiciones del sitio: información detallada sobre nuestros derechos de autor y marca comercial; su cuenta, licencia y acceso al sitio; y otros temas.

Historial de documentos

En esta página se enumeran los cambios importantes de esta documentación.

A veces, las funciones del servicio se implementan de forma gradual en AWS las regiones en las que el servicio está disponible. Actualizamos esta documentación solo para la primera versión. No proporcionamos información sobre la disponibilidad en regiones ni anunciamos lanzamientos posteriores en regiones. Para obtener información sobre la disponibilidad regional de las funciones del servicio y suscribirse a las notificaciones sobre actualizaciones, consulte ¿Qué hay de nuevo en el mercado? AWS .

Cambio	Descripción	Fecha
Reglas AWS gestionadas actualizadas para AWS WAF	Los grupos de reglas gestionados por Bot Control, ATP y ACFP ahora están versionados y proporcionarán notificaciones de SNS en caso de actualizaciones de versiones, al igual que otras reglas gestionadas AWS versionadas.	29 de mayo de 2024
Reglas AWS gestionadas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas del sistema operativo POSIX, `AWSManagedRulesUnixRuleSet` .	28 de mayo de 2024
CAPTCHAy Challenge acciones	Se ha añadido la aclaración de que los clientes de navegador es necesitan HTTPS para ejecutar puzles CAPTCHA y desafíos silenciosos.	24 de mayo de 2024
Integración con Amazon Security Lake	Ahora puede usar Security Lake para recopilar datos	22 de mayo de 2024

	de tráfico de ACL web. Para obtener más información, consulte Recopilación de datos de AWS los servicios en la guía del usuario de Amazon Security Lake.	
Reglas AWS gestionadas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas del conjunto de reglas principal (CRS).	21 de mayo de 2024
Reglas AWS gestionadas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas de la base de datos SQLi.	14 de mayo de 2024
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualiza r las entradas incorrectas conocidas y los grupos de reglas del sistema operativo POSIX.	8 de mayo de 2024
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas del sistema operativo Windows.	3 de mayo de 2024
AWS WAF Ejemplos de código de Kotlin para Android (SDK) para dispositivos móviles	Se agregó un código de ejemplo para las integraciones de Android basadas en Kotlin.	2 de mayo de 2024

AWS WAF métricas, dimensiones añadidas y métricas nuevas	AWS WAF se agregó una nueva dimensión para `ManagedRuleSetRule` las métricas de la regla y nuevas métricas para la acción de la regla coincidente para las métricas de etiquetas.	2 de mayo de 2024
AWS Firewall Manager admite las políticas de ACL de red	Firewall Manager ahora admite la administración de las listas de control de acceso (ACL) a la red de Amazon VPC a través de las políticas de ACL de red de Firewall Manager.	25 de abril de 2024
AWS Firewall Manager actualizaciones de la política de seguridad	Actualizaciones `FMSServiceRolePolicy` para agregar permisos para administrar las ACL de la red.	22 de abril de 2024
Lista actualizada de métricas de control de estado	Hemos eliminado algunas métricas de la lista de las que se utilizan habitualmente en los controles de estado.	16 de abril de 2024
Actualizaciones de las políticas de grupos de seguridad de Firewall Manager	Hemos actualizado nuestras políticas de auditoría de uso de los grupos de seguridad y mejorado la documenta ción. Consulte la sección de políticas de auditoría de uso y las secciones sobre mejores prácticas y limitaciones.	2 de abril de 2024

Ejemplos actualizados de control de bots	Se agregaron ejemplos que muestran el nivel de inspección objetivo y se actualizaron los ejemplos existentes para reflejar las mejores prácticas.	27 de marzo de 2024
Ejemplos de ATP actualizados	Se agregó un ejemplo que muestra la configuración de la inspección de respuesta y se actualizaron los ejemplos existentes para reflejar las mejores prácticas.	27 de marzo de 2024
Ejemplos de ACFP actualizados	Se agregó un ejemplo que muestra la configuración de la inspección de respuesta.	27 de marzo de 2024
Actualizar los límites de transmisión CloudWatch de registros de Amazon Logs	AWS WAF ya no tiene límites de ACL por web para publicar registros en las transmisiones de CloudWatch registros de Logs.	27 de marzo de 2024
AWS Shield Advanced protecciones de capa de aplicación (capa 7)	Guía general actualizada y de mejores prácticas para la detección y mitigación en la capa de aplicaciones, el uso de las ACL web, las reglas basadas en tasas y la mitigación automática de los ataques DDoS en la capa de aplicación.	14 de marzo de 2024
Reglas AWS gestionadas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas de reputación IP.	13 de marzo de 2024

Cambios en los límites de tamaño de la inspección corporal	AWS WAF ahora admite límites de tamaño más grandes para la inspección corporal en algunos recursos regionales.	7 de marzo de 2024
Ventana de evaluación configurable para reglas AWS WAF basadas en tarifas	Ahora puede configurar el intervalo de tiempo que utilizan las reglas basadas en tasas para contar las solicitud es, en 1, 2, 5 o 10 minutos. El valor predeterminado es 5, que era la única opción antes de esta versión.	28 de febrero de 2024
Información de registro ampliada para CAPTCHA y Challenge	El nivel superior `captchaResponse` y `challengeResponse` los campos ahora se rellenan con las últimas de estas acciones que se deben aplicar a una solicitud, ya sea finalizada o no. Antes, estos campos se rellenaban únicamente para las acciones de finalización.	22 de febrero de 2024
JavaScript Administración de claves de la API CAPTCHA	Ahora puede eliminar las claves de la API JS de CAPTCHA a través de las API. AWS WAF	6 de febrero de 2024
AWS WAF Audio de rompecabezas CAPTCHA	La versión en audio del rompecabezas CAPTCHA ahora es compatible con varios idiomas.	6 de febrero de 2024

AWS WAF desafío y etiquetado de tokens CAPTCHA	La administración de token ahora agrega etiquetas para el token CAPTCHA y ha mejorado el etiquetado de token para el de desafío.	20 de diciembre de 2023
Reglas AWS gestionadas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas de entradas incorrectas conocidas.	16 de diciembre de 2023
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas de entradas incorrectas conocidas.	14 de diciembre de 2023
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas del conjunto de reglas principal (CRS).	6 de diciembre de 2023
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas: AWS WAF Bot Control.	5 de diciembre de 2023
AWS Config Requisitos previos actualizados de Firewall Manager	Si utiliza un rol de IAM personalizado en lugar del rol administrado por Firewall Manager AWS Config, debe asegurarse de que su política de permisos permita a AWS Config Recorder grabar los recursos del Firewall Manager.	17 de noviembre de 2023

AWS WAF paneles de consola	Hemos corregido la guía para ver todas las reglas y muestras de solicitudes de una ACL web en la AWS WAF consola.	17 de noviembre de 2023
Se actualizaron las reglas AWS gestionadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas de control de bots.	14 de noviembre de 2023
AWS WAF la consola tiene nuevos paneles de ACL web	La página web de ACL de la AWS WAF consola tiene nuevos paneles de información general sobre el tráfico web.	14 de noviembre de 2023
Grupo de reglas administradas de ATP actualizado	Se ha corregido la información de las etiquetas de las reglas `VolumetricIpFailedLoginResponseHigh` y `VolumetricSessionFailedLoginResponseHigh` .	13 de noviembre de 2023
Grupo de reglas administradas de ACFP actualizado	Se ha corregido la información de las etiquetas de las reglas `VolumetricIPSuccessfulResponse` y `VolumetricSessionSuccessfulResponse` .	13 de noviembre de 2023
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas del conjunto de reglas principal (CRS).	2 de noviembre de 2023

Mitigación de DDoS de la capa de aplicación automática de Shield Advanced	Shield Advanced ahora mantiene una regla basada en tasas en el grupo de reglas de mitigación automática, que limita el volumen de solicitudes de direcciones IP conocidas por ser fuentes de ataques DDoS.	31 de octubre de 2023
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas del conjunto de reglas principal (CRS).	30 de octubre de 2023
El grupo de reglas administradas de control de bots ha eliminado la etiqueta de señal para el CSP de la solicitud	El grupo de reglas administrado por el control de bots ha eliminado la etiqueta de señal que indica el proveedor de servicios en la nube (CSP).	28 de octubre de 2023
Etiqueta de señal del grupo de reglas administradas de control de bots para el CSP de la solicitud	Las etiquetas de señal del grupo de reglas administrado por el control de bots incluye una etiqueta que indica el proveedor de servicios en la nube (CSP).	27 de octubre de 2023
Información de permisos AWS WAF de IAM actualizada	Para las AWS WAF acciones que gestionan las asociaciones de ACL web, la sección de acciones políticas ahora incluye los requisitos de permisos para cada tipo de recurso de aplicación web.	25 de octubre de 2023

Administración de Firewall Manager de ACL web modificadas	Al habilitar la administración de las ACL web no asociadas, el Firewall Manager no incluye las ACL web modificadas en la limpieza única de los recursos no utilizados.	19 de octubre de 2023
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas del sistema operativo POSIX,`AWSManagedRulesUnixRuleSet` .	12 de octubre de 2023
AWS WAF métricas, dimensiones añadidas	AWS WAF se agregaron nuevas dimensiones para ver las métricas de ACL web.	12 de octubre de 2023
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas del conjunto de reglas principal (CRS).	11 de octubre de 2023
Actualización de la especificación del SDK AWS WAF móvil	Se ha agregado la operación de `storeTokenInCookieStorage` a `WAFTokenProvider` .	11 de octubre de 2023
Implementaciones de excepciones: reglas AWS administradas para AWS WAF	AWS Managed Rules for AWS WAF publicó dos versiones estáticas del grupo de reglas conocido como entradas incorrectas y actualizó la versión predeterminada para que apuntara a la versión estática más reciente.	4 de octubre de 2023

AWS WAF La entidad HTML decodifica la transformación de texto	Se ha ampliado la funcionalidad de la transformación de texto de decodificación de entidades HTML.	4 de octubre de 2023
Se ha agregado una nueva opción a la política común del grupo de seguridad de Firewall Manager	Ahora Firewall Manager puede distribuir las referencias de los grupos de seguridad a los grupos de seguridad de réplicas.	3 de octubre de 2023
AWS WAF añade la inspección de la huella dactilar JA3	Ahora puedes realizar una comparación exacta con la huella digital JA3 de la solicitud web para CloudFront las distribuciones de Amazon y los balanceadores de carga de aplicaciones.	26 de septiembre de 2023
Actualizaciones de la configuración de reglas de políticas de grupos de seguridad de Firewall Manager	Firewall Manager ahora admite la referencia de grupos de seguridad desde los grupos de seguridad principales a los grupos de seguridad de réplicas.	25 de septiembre de 2023
Se ha actualizado la mitigación de DDoS de la capa de aplicación automática de Shield Advanced	Ahora Firewall Manager admite los recursos del equilibrador de carga de aplicación para las políticas de Shield Advanced configuradas con la mitigación automática de DDoS en la capa de aplicación.	14 de septiembre de 2023

Reglas administradas actualizadas AWS para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas: AWS WAF Bot Control.	6 de septiembre de 2023
AWS WAF Control de bots	Ahora el nivel de protección específico del grupo de reglas administradas del control de bots inspecciona la reutilización de los tokens entre direcciones IP. Ahora también ofrece un análisis opcional de las estadísticas de tráfico mediante machine learning (aprendizaje automático) para detectar alguna actividad relacionada con los bots.	6 de septiembre de 2023
Actualización de la especificación del SDK AWS WAF móvil	Se han reducido los valores mínimo, máximo y predeterminado de `tokenRefreshDelaySec` de mínimo 300, máximo 600 y el predeterminado 300 a mínimo 88, máximo 300 y predeterminado 88.	5 de septiembre de 2023
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas de control de AWS WAF bots.	30 de agosto de 2023

Mitigación de DDoS de la capa de aplicación automática de Shield Advanced	Se agregó una guía AWS CloudFormation para administrar las ACL web que se utilizan con la mitigación automática de DDoS en la capa de aplicación.	30 de agosto de 2023
Nueva opción de política de grupo de seguridad de auditoría de contenido de Firewall Manager	Se ha agregado una nueva opción para auditar grupos de reglas excesivamente permisivos y se han mejorado las descripciones de los procedimientos de la consola.	29 de agosto de 2023
Nueva opción de AWS WAF política y escudo de Firewall Manager	Si habilita la administración de ACL web no asociadas en AWS WAF and Shield, Firewall Manager solo crea ACL web en las cuentas dentro del ámbito de la política solo si las utilizará al menos un recurso.	9 de agosto de 2023
Se actualizaron las reglas administradas para AWSAWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas del conjunto de reglas principal (CRS).	26 de julio de 2023
Incorporación de reglas basadas en tasas en la ruta de URI	Ahora puede especificar la ruta de URI en sus claves de agregación personalizadas para las reglas basadas en tasas.	19 de julio de 2023

Nueva opción AWS WAF de regla de política en AWS Firewall Manager	AWS Firewall Manager añade soporte para configurar los límites de tamaño de inspección del cuerpo de las solicitudes AWS WAF web.	18 de julio de 2023
AWS WAF cambios de política gestionados	Se actualizó `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` , y `AWSWAFConsoleReadOnlyAccess` para añadir el acceso AWS verificado a los tipos de recursos con los que puede protegerse AWS WAF.	17 de junio de 2023
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF agregar el grupo de reglas`AWSManagedRulesACFPRuleSet` .	13 de junio de 2023
Actualización del control del AWS WAF fraude y la prevención de apropiación de cuentas (ATP)	Ya se puede especificar el punto de conexión de inicio de sesión para el grupo de reglas administrado ATP mediante una expresión regular.	13 de junio de 2023
Nueva información para la API CAPTCHA JavaScript	En la nueva sección se describe cómo resolver un rompecabezas de CAPTCHA personalizado cuando se AWS WAF responde a una solicitud con un CAPTCHA.	13 de junio de 2023

Nuevo grupo de reglas administradas de ACFP	Utilice el nuevo grupo de reglas `AWSManagedRulesACFPRuleSet` para detectar y bloquear los intentos fraudulentos de creación de cuentas.	13 de junio de 2023
Creación de nuevas cuentas de Control de AWS WAF Fraude y Prevención del Fraude (ACFP)	Puede detectar y bloquear los intentos fraudulentos de creación de cuentas con el nuevo grupo de reglas gestionado por AWS WAF Fraud Control y prevención del fraude en la creación de cuentas (ACFP). `AWSManagedRulesACFPRuleSet` Con CloudFront las distribuciones protegidas, también puedes usar la ACFP para bloquear los intentos de creación de nuevas cuentas por parte de clientes que recientemente hayan realizado demasiados intentos fallidos de creación de cuentas.	13 de junio de 2023
AWS WAF gestionó los cambios de política	Se actualizó `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` , y `AWSWAFConsoleReadOnlyAccess` para corregir la configuración de acceso a los AWS App Runner servicios.	6 de junio de 2023

Se ha agregado una limitación para las políticas de grupos de seguridad de Firewall Manager	Si posteriormente se deja de compartir una VPC compartida, Firewall Manager no eliminará los grupos de seguridad de réplica de la cuenta asociada.	2 de junio de 2023
Nuevo componente de AWS WAF solicitud: Header order	Ahora puede compararlos con una lista ordenada de los nombres de los encabezados de la solicitud.	30 de mayo de 2023
Reglas AWS gestionadas actualizadas para AWS WAF	Se ha actualizado el conjunto de reglas del sistema operativo Linux.	22 de mayo de 2023
Se actualizó la organización de la sección de AWS WAF reglas	Los listados de instrucciones de reglas ahora están agrupados por tipo de instrucción.	16 de mayo de 2023
Tema trasladado: lista de direcciones IP cuyas tasas están limitadas	El tema sobre la lista de direcciones IP cuyas tasas están limitadas por una regla basada en tasas se encuentra ahora en el tema de las reglas basadas en tasas.	16 de mayo de 2023

Opciones ampliadas para las reglas basadas en tasas	Ahora puede limitar la tasa de las solicitudes web en función de las claves de agregación distintas de las direcciones IP y puede agregarlas mediante combinaciones de claves. También puede limitar la tasa de todas las solicitudes que coincidan con una instrucción de restricción de acceso, sin necesidad de agregar más.	16 de mayo de 2023
Aumentos de la cuota de Firewall Manager	Se aumentó el número de políticas de Firewall Manager por organización AWS Organizations de 20 a 50. Aumento del número máximo de grupos de seguridad principales por política de uno a tres. Se ha cambiado el número máximo de WCU de una cuota flexible a una cuota fija.	5 de mayo de 2023
Aumento del número máximo de WCU por grupo de reglas	Ahora se pueden utilizar hasta 5000 unidades de capacidad de ACL web (WCU) por grupo de reglas sin solicitar un aumento de la compatibilidad. Este nuevo límite no se puede aumentar.	1 de mayo de 2023
AWS WAF Ubicaciones de depósitos de registro de Amazon S3 con prefijos	AWS WAF ahora permite prefijos en los nombres de los buckets de registro de Amazon S3.	1 de mayo de 2023

Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas del conjunto de reglas principal (CRS).	28 de abril de 2023
Se agregó soporte para instancias de acceso AWS verificado a AWS WAF	Ahora puede asociar una ACL AWS WAF web a una instancia de acceso verificado. Este cambio solo está disponible en la versión más reciente de AWS WAF , no en la versión AWS WAF clásica.	28 de abril de 2023
Capítulo revisado sobre el trabajo con varios administradores de Firewall Manager	Ahora se pueden designar varios administradores de Firewall Manager para crear y administrar los recursos de firewall de una organización.	24 de abril de 2023
AWS Firewall Manager actualización de política gestionada	Actualizado `FMSServiceRolePolicy` .	21 de abril de 2023
Nueva integración de aplicaciones JavaScript cliente para CAPTCHA	Ahora puede personalizar la ubicación y las características del rompecabezas CAPTCHA en sus aplicaciones cliente. JavaScript	20 de abril de 2023

La integración de aplicaciones ha pasado a denominarse integración inteligente de amenazas	Hemos cambiado el nombre de la funcionalidad existente para la integración de aplicaciones cliente por la de integraciones de amenazas inteligentes, a fin de poder distinguirla de la nueva integración de aplicaciones CAPTCHA. JavaScript	20 de abril de 2023
Precios variables para las WCU de ACL web superiores a 1500	El uso de más de 1500 unidades de capacidad de ACL web (WCU) en su ACL web implica costos adicionales, que se ajustan automáticamente a medida que aumenta o disminuye el uso de la WCU de ACL web. El máximo de ACL web es de 5000 WCU.	11 de abril de 2023
Aumento del número máximo de WCU por ACL web	Ahora se pueden utilizar hasta 5000 unidades de capacidad de ACL web (WCU) por ACL web sin solicitar un aumento de la compatibilidad. Este nuevo límite no se puede aumentar.	11 de abril de 2023
Límites de tamaño para la inspección corporal de las ACL web CloudFront	En el caso de las ACL web que protegen CloudFront las distribuciones de Amazon, puede aumentar el límite de tamaño de la inspección corporal hasta 64 KB en su configuración de ACL web.	11 de abril de 2023

Aumento del tamaño de la inspección corporal para CloudFront	El límite máximo de tamaño de inspección AWS WAF corporal para CloudFront las distribuciones de Amazon se incrementó de 8 KB a 64 KB. El límite de tamaño de inspección predeterminado CloudFront es de 16 KB.	11 de abril de 2023
Nuevas opciones AWS WAF de reglas políticas en AWS Firewall Manager	AWS Firewall Manager añade compatibilidad con los grupos de reglas de prevención de apropiación de cuentas (ATP) y AWS WAF Bot Control AWS Managed Rules de AWS WAF Fraud Control, los destinos de registro de Amazon S3, las anulaciones de acciones de reglas y las acciones de `Challenge` reglas, `CAPTCHA` y las listas de dominios simbólicos.	7 de abril de 2023
Firewall Manager admite buckets de Amazon S3 como destinos de registro para el AWS WAF registro	Ahora puede usar los buckets de Amazon S3 como destinos de registro en sus AWS WAF políticas.	7 de abril de 2023

AWS WAF ha gestionado los cambios de política	Se actualizó `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` `AWSWAFReadOnlyAccess` , y `AWSWAFConsoleReadOnlyAccess` para añadir AWS App Runner servicios a los tipos de recursos con los que puede protegerse AWS WAF.	30 de marzo de 2023
Se ha agregado una advertencia sobre el uso de etiquetas en las políticas de los grupos de seguridad	Firewall Manager no actualizará las etiquetas de los grupos de seguridad existentes ni creará nuevos grupos de seguridad si la política tiene etiquetas que entren en conflicto con la política de etiquetas de la organización.	28 de marzo de 2023
Actualización de la información sobre roles de servicio	Se ha actualizado la forma de usar un rol de servicio con Firewall Manager.	8 de marzo de 2023
Se ha corregido la información sobre cómo las reglas basadas en tasas limitan las tasas	Las reglas basadas en tasas con instrucciones de restricción de acceso solo limitan las tasas de las solicitudes que coinciden con la instrucción de restricción de acceso. Decíamos que el límite se aplicaba a todas las solicitudes de cualquier dirección IP con tasa limitada.	1 de marzo de 2023

Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas de la aplicación PHP.	27 de febrero de 2023
Se agregó soporte AWS App Runner para AWS WAF	Ahora puede asociar una ACL AWS WAF web a un AWS App Runner servicio. Este cambio solo está disponible en la versión más reciente de AWS WAF , no en la versión AWS WAF clásica.	23 de febrero de 2023
Se actualizó la guía de IAM para AWS Firewall Manager	Se ha actualizado la guía para implementar las prácticas recomendadas de IAM. Para obtener más información, consulte prácticas recomendadas de seguridad en IAM.	16 de febrero de 2023
Se actualizaron las reglas AWS gestionadas para AWS WAF	AWS Managed Rules for AWS WAF actualizó el grupo de reglas `AWSManagedRulesATPRuleSet` para añadir la inspección de las respuestas de inicio de sesión en las ACL web que protegen las CloudFront distribuciones de Amazon.	15 de febrero de 2023

AWS WAF Inspección de respuesta al inicio de sesión y prevención de apropiación de cuentas (ATP) de Fraud Control	En el caso de CloudFront las distribuciones protegidas, ahora puede usar ATP para bloquear los nuevos intentos de inicio de sesión de los clientes que recientemente han realizado demasiados intentos fallidos de inicio de sesión.	15 de febrero de 2023
Reglas AWS administradas actualizadas para AWS WAF	Se ha actualizado el conjunto de reglas básicas.	25 de enero de 2023
Las prácticas recomendadas para la mitigación inteligente de amenazas	Se ha agregado una sección con las prácticas recomenda das para implementar el control de bots, la ATP y otras características inteligentes de mitigación de amenazas.	22 de enero de 2023
Cómo inspeccionar los pseudoencabezados de HTTP/2	Se ha agregado una sección que asigna los pseudoenc abezados de HTTP/2 a sus componentes de solicitud web correspondientes.	20 de enero de 2023
Se actualizó la guía de IAM para AWS WAF la versión clásica	Se ha actualizado la guía para implementar las prácticas recomendadas de IAM. Para obtener más información, consulte prácticas recomenda das de seguridad en IAM.	3 de enero de 2023

Se actualizó la guía de IAM para AWS WAF	Se ha actualizado la guía para implementar las prácticas recomendadas de IAM. Para obtener más información, consulte prácticas recomendadas de seguridad en IAM.	3 de enero de 2023
Se actualizó la guía de IAM para AWS Shield	Se ha actualizado la guía para implementar las prácticas recomendadas de IAM. Para obtener más información, consulte prácticas recomendadas de seguridad en IAM.	3 de enero de 2023
Actualización de las políticas DNS Firewall de Amazon Route 53 Resolver	Se ha agregado información sobre la eliminación de grupos de reglas de DNS Firewall de Amazon Route 53 Resolver.	29 de diciembre de 2022
Se actualizaron las reglas AWS gestionadas para AWS WAF	Se ha actualizado el conjunto de reglas del sistema operativo Linux.	15 de diciembre de 2022
Reglas AWS gestionadas actualizadas para AWS WAF	Se ha actualizado el conjunto de reglas básicas.	5 de diciembre de 2022
Firewall Manager agrega compatibilidad para firewall nativo en la nube (CNF) de Fortigate como políticas de servicio	Firewall Manager ahora es compatible con las políticas de Fortigate CNF.	2 de diciembre de 2022
Se ha eliminado AWS Config el requisito de las políticas de firewall de DNS	Para las políticas de firewall de DNS, ahora solo se necesita habilitar Config para el tipo de recurso VPC de EC2.	17 de noviembre de 2022

AWS Firewall Manager actualización de políticas gestionada	Actualizado `FMSServiceRolePolicy` .	15 de noviembre de 2022
Ampliación de las opciones de idioma para el rompecabezas AWS WAF CAPTCHA	El rompecabezas CAPTCHA ahora ofrece sus instrucciones escritas en varios idiomas. Las instrucciones incluidas en cada rompecabezas de audio siguen estando disponibles únicamente en inglés.	11 de noviembre de 2022
Nuevas cuotas de Firewall Manager para los conjuntos de recursos	Se han agregado nuevas cuotas para los conjuntos de recursos.	8 de noviembre de 2022
Agregar compatibilidad para conjuntos de recursos	Puede crear conjuntos de recursos para agrupar los recursos y administrarlos en una política de Firewall Manager.	8 de noviembre de 2022
Agregar compatibilidad para importar firewalls desde Network Firewall	Ahora puede importar y administrar los firewalls existentes en las políticas de Network Firewall mediante conjuntos de recursos.	8 de noviembre de 2022
AWS Firewall Manager actualización gestionada de la política	Actualizado `AWSFMAdminReadOnlyAccess` .	2 de noviembre de 2022
La instrucción de coincidencia geográfica ahora agrega etiquetas a las solicitudes de país y región	Ahora puede administrar los orígenes geográficos de las solicitudes a nivel de región combinando la coincidencia geográfica con la coincidencia de etiquetas.	31 de octubre de 2022

Cambió de nombre de la sección de nivel superior: protecciones administradas	La sección ahora se denomina mitigación AWS WAF inteligente de amenazas, que coincide con nuestras páginas de marketing.	27 de octubre de 2022
Nuevo nivel de protección objetivo en el grupo de reglas administradas del control de bots	El grupo de reglas administrado de control de bots ahora ofrece reglas específicas adicionales para la detección y mitigación de bots sofisticados. Este nivel de protección está disponible por una tarifa adicional.	27 de octubre de 2022
Nueva sección sobre fichas AWS WAF	Comprenda cómo se AWS WAF utilizan los tokens para la mitigación inteligente de amenazas.	27 de octubre de 2022
Se ha agregado una nota importante sobre la actualización de las políticas de Network Firewall de Firewall Manager	Al actualizar una política de Firewall Manager, todas las políticas de Network Firewall creadas por la política se actualizarán con la configuración de políticas de Network Firewall de la política de Firewall Manager.	27 de octubre de 2022

Anulaciones de acciones en los grupos de reglas	Ahora puede anular las acciones de las reglas de un grupo de reglas en cualquier configuración de acciones de reglas. Al igual que con la anulación de la acción Count anterior, puede aplicar las anulaciones a todas las reglas de un grupo de reglas y a reglas individuales.	27 de octubre de 2022
AWS WAF nueva Challenge regla, opción de acción	Puede configurar las reglas para usar un Challenge y así comprobar si los navegadores envían las solicitudes.	27 de octubre de 2022
AWS WAF permite compartir los tokens entre varias aplicaciones protegidas	Puede habilitar el uso de tokens en varias aplicaciones protegidas configurando una lista de dominios de tokens para su ACL web.	27 de octubre de 2022
Ninguna especificación de encabezados distingue entre mayúsculas y minúsculas	Se ha modificado la especific ación de todos los encabezad os para que no distinga entre mayúsculas y minúscula s. Esto coincide con el comportamiento de un encabezado único.	26 de octubre de 2022
AWS Firewall Manager gestionó los cambios de política	Correcciones a `AWSFMAdmi nFullAccess` .	21 de octubre de 2022
Reglas AWS gestionadas actualizadas para AWS WAF	Se ha actualizado el grupo de reglas de entradas incorrectas conocidas.	20 de octubre de 2022

Reglas AWS gestionadas actualizadas para AWS WAF	Se ha actualizado el grupo de reglas de entradas incorrectas conocidas.	5 de octubre de 2022
Actualización de la especificación del SDK AWS WAF móvil	Se ha reducido el valor predeterminado de `tokenRefreshDelaySec` de 600 (10 minutos) a 300 (5 minutos).	30 de septiembre de 2022
Reglas AWS administradas actualizadas para AWS WAF	Se corrigieron los nombres de las etiquetas proporcionados en esta documentación para los siguientes grupos de reglas: sistema operativo POSIX, aplicación PHP y WordPress aplicación.	19 de septiembre de 2022
Nueva opción AWS WAF de regla de política en AWS Firewall Manager	AWS Firewall Manager ahora admite solicitudes y respuestas web personalizadas para las acciones web predeterminadas en AWS WAF las políticas.	9 de septiembre de 2022
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas: reputación IP.	30 de agosto de 2022

AWS WAF cambios de política gestionados	Se actualizó `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` , y `AWSWAFConsoleReadOnlyAccess` para añadir grupos de usuarios de Amazon Cognito a los tipos de recursos con los que puede protegerse. AWS WAF	25 de agosto de 2022
AWS WAF Control de fraudes y prevención de apropiación de cuentas (ATP)	Ahora puedes usar la función de prevención de apropiación de cuentas (ATP) de AWS WAF Fraud Control con las CloudFront distribuciones de Amazon.	24 de agosto de 2022
Reglas AWS gestionadas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas: Entradas incorrectas conocidas.	22 de agosto de 2022
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas:`AWSManagedRulesATPRuleSet` .	11 de agosto de 2022

Se ha añadido compatibilidad con los grupos de usuarios de Amazon Cognito a AWS WAF	Ahora puede asociar una ACL AWS WAF web a un grupo de usuarios de Amazon Cognito. Este cambio solo está disponible en la versión más reciente de AWS WAF , no en la versión AWS WAF clásica.	11 de agosto de 2022
Se agregó una sección sobre las implementaciones de grupos de reglas de reglas AWS administradas versionados	Se agregó una nueva sección que documenta las implementaciones de grupos de reglas de reglas administradas versionados AWS . La sección incluye información sobre cómo se nombran las versiones predeterminadas durante las implementaciones de las versiones candidatas.	29 de julio de 2022
Requisitos actualizados para configurar el registro para las políticas de Network Firewall	Se han agregado requisitos para las políticas de Network Firewall que utilizan un bucket de Amazon S3 cifrado como destino del registro.	26 de julio de 2022
Opción de nivel de sensibilidad para la instrucción de regla SQLi	Ahora puede aumentar la sensibilidad de sus instrucciones de reglas de inyección de código SQL. Esto no cambia el comportamiento de las instrucciones existentes, cuyo nivel de sensibilidad predeterminado es LOW.	15 de julio de 2022

Se ha agregado la opción de configuración de políticas de Network Firewall	Ahora Firewall Manager admite el orden de evaluación con estado y las acciones predeterminadas en las configuraciones de políticas de firewall de Network Firewall.	14 de julio de 2022
Actualizaciones de la configuración de reglas de políticas de grupos de seguridad de Firewall Manager	Firewall Manager ahora admite la distribución de etiquetas de los grupos de seguridad principales a los grupos de seguridad de réplicas.	7 de julio de 2022
Actualizaciones de la guía AWS Shield	Se ha ampliado la información de la guía de Shield para describir cómo Shield mitiga los eventos.	24 de junio de 2022
Guía actualizada para probar y ajustar AWS WAF las protecciones	La guía general para las pruebas y el ajuste AWS WAF se ha actualizado y ahora es un tema de primer nivel.	20 de junio de 2022
Reglas AWS gestionadas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas: conjunto de reglas básicas (CRS).	9 de junio de 2022
Nueva guía de suplentes confusos de Firewall Manager	Se agregó una guía sobre cómo evitar el problema de los suplentes confusos en Firewall Manager.	1 de junio de 2022

Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas: conjunto de reglas básicas (CRS).	24 de mayo de 2022
Nuevos componentes AWS WAF de solicitud: Headers y Cookies	Ahora puede inspeccionar las cookies de una solicitud web y puede inspeccionar todos los encabezados de una solicitud web, además de un solo encabezado.	29 de abril de 2022
AWS WAF manejo de componentes sobredimensionados del cuerpo, los encabezados y las solicitudes de cookies	Ahora puede especificar cómo se AWS WAF deben gestionar los cuerpos de las solicitudes, los encabezados y las cookies sobredimensionados en las reglas que inspeccionan estos componentes. Las reglas que ya ha creado para inspeccionar estos componentes tienen un comportamiento que coincide con la nueva opción de Continue de gestión del sobredimensionamiento.	29 de abril de 2022
AWS WAF Cambios en la política de registro de Amazon S3	Se han actualizado la política y el ejemplo de permisos de registro de Amazon S3.	12 de abril de 2022

La opción de mitigación automática de DDoS en la capa de aplicación ahora está disponible con AWS Shield Advanced Application Load Balancer	Shield Advanced ahora admite la mitigación de DDoS de la capa de aplicación automática para los equilibradores de carga de aplicaciones, por lo que está disponible para todas las protecciones de la capa de aplicación. Puede configurar Shield Advanced para que cuente o bloquee automáticamente las solicitudes web que forman parte de un ataque DDoS de la capa de aplicación contra un recurso protegido.	8 de abril de 2022
Se ha agregado un indicador de la configuración de versión predeterminada actual para los grupos de reglas administradas	Las listas de versiones de los grupos de reglas administradas ahora indican qué versión es la predeterminada actual.	8 de abril de 2022
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas: AWS WAF Bot Control.	6 de abril de 2022
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas: Entradas incorrectas conocidas.	31 de marzo de 2022
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas: Entradas incorrectas conocidas.	30 de marzo de 2022

Firewall Manager añade la compatibilidad con el firewall de próxima generación (NGFW) en la nube de Palo Alto Networks	Firewall Manager ahora es compatible con el Palo Alto Networks Cloud Next Generation Firewall (NGFW).	30 de marzo de 2022
Agregue soporte para el NGFW en la nube de Palo Alto Networks a AWS Firewall Manager	AWS Firewall Manager ahora es compatible con las políticas de firewall de próxima generación (NGFW) de Palo Alto Networks Cloud.	30 de marzo de 2022
Actualizaciones de la guía AWS Shield	Se ha ampliado la informaci ón de la guía de Shield para describir cómo Shield realiza la detección de eventos y proporcionar ejemplos de arquitecturas resistentes a los DDoS.	16 de marzo de 2022
Actualizaciones de la AWS Shield guía	Se ha ampliado la información de la guía de Shield y se ha mejorado la organización de varias secciones. Los principal es cambios se encuentran en las siguientes secciones de la guía Shield: compatibilidad con el equipo de respuesta de Shield (SRT), protección de recursos en AWS Shield Advanced y visibilidad de los eventos de DDoS.	28 de febrero de 2022

Firewall Manager ahora es compatible con el modelo de implementación centralizada de Network Firewall	Se ha agregado un nuevo procedimiento que explica cómo configurar políticas que utilicen modelos de implement ación distribuidos y centraliz ados.	24 de febrero de 2022
Firewall Manager añade soporte para el modelo de implementación AWS Network Firewall centralizada	Ahora puede configurar sus AWS Network Firewall políticas para usar el modelo de implementación distribui da o centralizada. Con el modelo de implementación distribuida, Firewall Manager crea y mantiene puntos de conexión de firewall en cada VPC que se encuentre dentro del alcance de la política. Con el modelo de implementación centralizada, Firewall Manager crea y mantiene los puntos de conexión del firewall en una sola VPC de inspección.	24 de febrero de 2022
Añada compatibilidad con el control de versiones de grupos de reglas AWS WAF gestionados a AWS Firewall Manager	AWS Firewall Manager ahora admite el control de versiones de grupos de reglas AWS WAF administrado en AWS WAF las políticas de Firewall Manager.	18 de febrero de 2022
AWS Firewall Manager cambio de política gestionado	Actualice a `FMSServiceRolePolicy` .	16 de febrero de 2022

Reglas AWS gestionadas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas: listas de reputación de IP.	15 de febrero de 2022
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF agregar el grupo `AWSManagedRulesATPRuleSet` de reglas de control de AWS WAF fraude y prevención de apropiación de cuentas (ATP).	11 de febrero de 2022
Cambios en la organización de la guía AWS WAF	Se ha agregado una nueva sección de nivel superior para las protecciones administradas. Se ha trasladado la sección de CAPTCHA de la sección dedicada a las reglas a la nueva sección de protecciones gestionadas. Se ha trasladado la sección de etiquetas de la sección dedicada a las reglas a su propia sección de nivel superior.	11 de febrero de 2022
AWS WAF integraciones de aplicaciones cliente	Utilice las API de clientes móviles AWS WAF JavaScript y las API para clientes móviles para integrar las aplicaciones de sus clientes con los grupos de reglas inteligentes de mitigación de amenazas AWS gestionadas para mejorar la detección.	11 de febrero de 2022

AWS WAF Control del fraude y prevención de apropiación de cuentas (ATP)	Puede detectar y bloquear los intentos de apropiación de cuentas con el nuevo grupo de reglas gestionado por AWS WAF Fraud Control para la prevención de apropiación de cuentas (ATP). `AWSManagedRulesATPRuleSet`	11 de febrero de 2022
Reglas AWS gestionadas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas: Entradas incorrectas conocidas.	28 de enero de 2022
AWS WAF cambios de política gestionados	Actualización de `AWSWAFFullAccessPolicy` y `AWSWAFConsoleFullAccess` para corregir los permisos de registro.	11 de enero de 2022
Reglas AWS gestionadas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas: conjunto de reglas básicas (CRS) y base de datos SQLi.	10 de enero de 2022
Firewall Manager admite la mitigación de DDoS de la capa de aplicación automática de Shield Advanced	Las políticas avanzadas de Firewall Manager Shield para CloudFront los recursos de Amazon ahora incluyen soporte para la mitigación automática de DDoS en la capa de aplicación.	7 de enero de 2022
AWS Firewall Manager cambio de política gestionado	Actualice a `FMSServiceRolePolicy` .	7 de enero de 2022

Reglas AWS gestionadas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas: Entradas incorrectas conocidas.	17 de diciembre de 2021
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas: Entradas incorrectas conocidas.	11 de diciembre de 2021
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas: Entradas incorrectas conocidas.	10 de diciembre de 2021
Nuevo rol AWS Shield Advanced vinculado a un servicio	Se ha agregado `AWSServiceRoleForAWSShield` para admitir la funcionalidad de mitigación automática de DDoS en la capa de aplicación.	1 de diciembre de 2021
Nueva política gestionada AWS Shield	Se ha agregado `AWSShieldServiceRolePolicy` para admitir la funcionalidad de mitigación automática de DDoS en la capa de aplicación.	1 de diciembre de 2021

La opción automática de mitigación de DDoS en la capa de aplicación ahora está disponible con AWS Shield Advanced CloudFront	Shield Advanced ahora admite la mitigación automática de DDoS en la capa de aplicación para las CloudFront distribuciones de Amazon. Puede configurar Shield Advanced para que cuente o bloquee automáticamente las solicitudes web que forman parte de un ataque DDoS de capa de aplicación contra una CloudFront distribución.	1 de diciembre de 2021
Reglas AWS gestionadas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los siguientes grupos de reglas: conjunto de reglas principales (CRS), sistema operativo Windows, sistema operativo Linux y listas de reputación de IP.	23 de noviembre de 2021
AWS Firewall Manager cambio de política gestionado	Actualice a `FMSServiceRolePolicy` .	18 de noviembre de 2021
Opciones de registro ampliadas para AWS WAF	Ahora puede registrar el tráfico de ACL web en un grupo de CloudWatch registros de Amazon Logs o en un bucket de Amazon Simple Storage Service (Amazon S3). Estas opciones se suman a la opción existente de iniciar sesión en una transmisión de entrega de Amazon Data Firehose.	15 de noviembre de 2021

AWS WAF cambios de política gestionados	Actualización de `AWSWAFFullAccessPolicy` y `AWSWAFConsoleFullAccess` para admitir destinos de registro adicionales.	15 de noviembre de 2021
AWS WAF nueva opción de acción de CAPTCHA regla	Puede configurar reglas para ejecutar un CAPTCHA en las solicitudes web y, según sea necesario, enviar un problema de CAPTCHA al cliente.	8 de noviembre de 2021
Reglas AWS gestionadas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas del conjunto de reglas principal (CRS).	27 de octubre de 2021
Reglas AWS administradas actualizadas para AWS WAF	Todos los grupos de reglas de reglas AWS administradas ahora admiten el etiquetado. Las descripciones de las reglas incluyen las especificaciones de la etiqueta.	25 de octubre de 2021
Firewall Manager admite el filtrado de registros de Network Firewall	AWS Firewall Manager ahora admite el filtrado de registros para las políticas de Network Firewall.	4 de octubre de 2021
AWS Firewall Manager cambio de política gestionado	Actualice a `FMSServiceRolePolicy` .	29 de septiembre de 2021
Se ha agregado una instrucción de coincidencia de regex	Ahora puede hacer coincidir las solicitudes web con una sola expresión regular.	22 de septiembre de 2021

Reglas basadas en tasas dentro de los grupos de AWS WAF reglas	Ahora puede definir reglas basadas en tasas dentro AWS WAF de los grupos de reglas. En AWS Firewall Manager, esta capacidad es totalmente compatible con las AWS WAF políticas.	13 de septiembre de 2021
Firewall Manager admite el filtrado de AWS WAF registros	AWS Firewall Manager ahora admite el filtrado de registros para AWS WAF las políticas.	31 de agosto de 2021
Elimine automáticamente las protecciones out-of-scope de recursos en AWS Firewall Manager	AWS Firewall Manager le permite eliminar automátic amente las protecciones de los recursos que están fuera del ámbito de aplicación de la política.	25 de agosto de 2021
AWS Firewall Manager cambio de política gestionado	Actualice a `FMSServiceRolePolicy` .	12 de agosto de 2021
Se ha agregado el control de versiones a los grupos de reglas administradas	Los proveedores de grupos de reglas administradas ahora pueden crear versiones de sus grupos de reglas.	9 de agosto de 2021
Modificar los requisitos AWS Firewall Manager de administrador	Puede usar la cuenta de administración de la organización como cuenta de administrador de Firewall Manager. Esta opción no estaba autorizada.	2 de agosto de 2021

Aumento de la cuota de Firewall Manager	Aumento del número de instancias de Amazon VPC que puede tener en el alcance de una política de Firewall Manager de 10 a 100.	28 de julio de 2021
AWS Firewall Manager soporte para la supervisión de tablas de AWS Network Firewall enrutamiento	AWS Firewall Manager ahora admite la supervisión de tablas de enrutamiento y proporcio na recomendaciones de medidas correctivas a los administradores de seguridad para AWS Network Firewall las políticas con rutas mal configuradas.	8 de julio de 2021
AWS WAF opciones adicional es de transformación de texto	Se han ampliado las opciones para las transformaciones de texto, que se pueden aplicar a los componentes de las solicitudes web antes de inspeccionarlos.	24 de junio de 2021
Se modificó la denominación de los recursos de AWS WAF políticas de Firewall Manager	El nombre de las ACL web, los grupos de reglas y los registros que el Firewall Manager administra para sus AWS WAF políticas ha cambiado.	26 de mayo de 2021

Reglas AWS administradas actualizadas para AWS WAF	AWS Managed Rules para AWS WAF añadir compatibilidad con el etiquetado en las listas de reputación IP y eliminar los sufijos de los nombres de las reglas para la lista de reputación IP de Amazon.	4 de mayo de 2021
Añada compatibilidad con el administrador AWS Organizations delegado	Al configurar la cuenta de AWS Firewall Manager administrador, el Administrador de Firewall ahora designa la cuenta como administrador AWS Organizations delegado de Firewall Manager. Con este cambio, al configurar la cuenta de administrador del Firewall Manager, se debe proporcionar una cuenta de miembro distinta a la cuenta de administración de la organización. Este cambio no afecta a su configuración actual.	30 de abril de 2021
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF agregar el grupo de reglas de control de AWS WAF bots.	1 de abril de 2021

Definir las acciones de las reglas individuales en un grupo de reglas Count	Ahora puede definir las acciones de las reglas individuales a Count en un grupo de reglas. Se ha corregido la información de la anulación existente, que se encuentra en el nivel del grupo de reglas.	1 de abril de 2021
Instrucción de restricción de acceso para los grupos de reglas administradas	Ahora puede usar una instrucción de restricción de acceso con los grupos de reglas administrados de la misma manera que con una instrucción basada en tasas.	1 de abril de 2021
Filtrado de registros	Ahora puede filtrar el tráfico de ACL web que se registra en función de la acción y la etiqueta de la regla.	1 de abril de 2021
AWS WAF etiquetas en las solicitudes web	Puede configurar reglas para agregar etiquetas a las solicitudes web coinciden tes y para hacer coincidir las etiquetas agregadas por otras reglas.	1 de abril de 2021

AWS WAF Control de bots	Puedes supervisar y controlar el tráfico de bots con la nueva función de control de AWS WAF bots, que combina el grupo de reglas gestionado por el control de bots con el etiquetado de las solicitudes web, las declaraciones de alcance reducido y el filtrado de registros.	1 de abril de 2021
Firewall Manager es compatible con las políticas del Firewall de DNS de Amazon Route 53 Resolver	AWS Firewall Manager admite la administración centralizada del filtrado del tráfico DNS saliente del Firewall DNS de Amazon Route 53 Resolver para sus VPC.	31 de marzo de 2021
Gestión de solicitudes y respuestas personalizadas	Puede incluir encabezados personalizados para las solicitudes web que AWS WAF no bloquee y enviar respuestas personalizadas para las solicitudes web que AWS WAF bloquee. Está disponible para la configuración de acción predeterminada de ACL web y acción de regla.	29 de marzo de 2021
AWS Firewall Manager cambio de política gestionado	Actualice a `FMSServiceRolePolicy` .	17 de marzo de 2021

Reglas AWS gestionadas actualizadas para AWS WAF	AWS Managed Rules para AWS WAF actualizar los siguientes grupos de reglas: conjunto de reglas básicas (CRS), protección administrativa, entradas incorrectas conocidas y sistema operativo Linux.	3 de marzo de 2021
AWS Shield seguimiento gestionado de los cambios en las políticas	Shield comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	3 de marzo de 2021
AWS Firewall Manager gestionó el seguimiento de los cambios de políticas	Firewall Manager comenzó a rastrear los cambios de sus políticas AWS administradas.	2 de marzo de 2021
AWS WAF gestionó el seguimiento de los cambios de políticas	AWS WAF comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	1 de marzo de 2021
Inspeccionar el cuerpo de una solicitud web como JSON analizado	Se ha agregado la opción de inspeccionar el cuerpo de la solicitud web como JSON analizado y filtrado. Esto se suma a la opción existente para inspeccionar el cuerpo de la solicitud web como texto sin formato.	12 de febrero de 2021
Firewall Manager admite AWS Network Firewall políticas	AWS Firewall Manager admite la administración centralizada del filtrado del tráfico de AWS Network Firewall red para sus VPC.	17 de noviembre de 2020

Añada soporte para grupos de AWS Shield Advanced protección	Ahora se pueden agrupar los recursos protegidos en grupos lógicos y administrar sus protecciones de forma colectiva.	13 de noviembre de 2020
Se agregó soporte AWS AppSync para AWS WAF	Ahora puedes asociar una ACL AWS WAF web a tu API de AWS AppSync GraphQL. Este cambio solo está disponible en la última versión de AWS WAF , no en la versión AWS WAF clásica.	1 de octubre de 2020
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el conjunto de reglas del sistema operativo Windows.	23 de septiembre de 2020
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los conjuntos de reglas, la aplicación PHP y el sistema operativo POSIX.	16 de septiembre de 2020
Consola actualizada AWS Shield	AWS Shield ofrece una nueva opción de consola, con una experiencia de usuario mejorada. La guía de la consola que aparece en la documentación es para la nueva consola.	1 de septiembre de 2020

Firewall Manager se actualiza a las políticas comunes del grupo de seguridad	AWS Firewall Manager Las políticas comunes de los grupos de seguridad ahora admiten los tipos de recursos Application Load Balancers y Classic Load Balancers mediante la implementación de la consola. Las nuevas opciones están disponibles en la configuración del Alcance de la política de la política común.	11 de agosto de 2020
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el conjunto de reglas principales.	7 de agosto de 2020
Firewall Manager admite la configuración de AWS WAF registros	AWS Firewall Manager ahora admite la configuración de registro centralizada para AWS WAF las políticas.	30 de julio de 2020
Especificar la ubicación de la dirección IP en la solicitud web	Se ha agregado la opción de usar direcciones IP de un encabezado HTTP que especifique, en lugar de usar el origen de la solicitud web. Normalmente, el encabezado alternativo es `X-Forwarded-For` (XFF), pero puede especificar cualquier nombre de encabezado. Puede usar esta opción para la coincidencia de conjuntos de IP, la coincidencia geográfica y la agregación de recuentos de reglas basadas en tasas.	9 de julio de 2020

Firewall Manager se actualiza a las políticas del grupo de seguridad de auditoría de contenido	AWS Firewall Manager ha ampliado la funcionalidad para auditar el contenido de las políticas de los grupos de seguridad, incluida una opción de reglas administradas, que utiliza listas de aplicaciones y protocolos gestionados y detalles sobre las infracciones de recursos.	7 de julio de 2020
Listas administradas por Firewall Manager	AWS Firewall Manager ahora es compatible con las listas de aplicaciones y protocolos gestionados. Firewall Manager administra algunas listas y puede crear y administrar las suyas propias.	7 de julio de 2020
Firewall Manager admite VPC compartidas en políticas de grupos de seguridad comunes	AWS Firewall Manager ahora admite el uso de políticas de grupos de seguridad comunes en VPC compartidas. Puede hacerlo además de usarlas en las VPC que pertenecen a las cuentas dentro del ámbito.	26 de mayo de 2020
Reglas AWS administradas actualizadas para AWS WAF	Se agregó documentación para cada regla en las reglas AWS administradas para AWS WAF.	20 de mayo de 2020
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar el grupo de reglas del sistema operativo Linux.	19 de mayo de 2020

Añada compatibilidad para migrar los recursos de la AWS WAF versión clásica a la versión AWS WAF (v2)	Ahora puede usar la consola o la API para exportar sus recursos AWS WAF clásicos y migrarlos a la versión más reciente de AWS WAF.	27 de abril de 2020
Agregue soporte para las unidades AWS Organizations organizativas en el ámbito de las políticas	AWS Firewall Manager ahora admite el uso de unidades AWS Organizations organizativas (OU) para especificar el alcance de la política. Puede usar unidades organizativas para incluir o excluir cuentas del ámbito, además de incluir o excluir cuentas específicas. Especificar una unidad organizativa es lo mismo que especificar todas las cuentas de la unidad organizativa y de cualquiera de sus unidades organizativas secundarias, incluidas las unidades organizativas secundarias y las cuentas añadidas posteriormente.	6 de abril de 2020
Agregue soporte para AWS WAF (v2) a AWS Firewall Manager	AWS Firewall Manager ahora es compatible con la última versión de AWS WAF Classic AWS WAF, además de la versión anterior.	31 de marzo de 2020

Actualización de las políticas AWS Firewall Manager comunes de los grupos de seguridad	AWS Firewall Manager La política común de grupos de seguridad ahora tiene la opción de aplicar la política a todas las interfaces de red elásticas de las instancias Amazon EC2 incluidas en el ámbito. Aún puede elegir aplicar únicamente la política a la interfaz de red elástica predeterminada.	11 de marzo de 2020
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF agregar un grupo de `AWSManagedRulesAnonymousIpList` reglas.	6 de marzo de 2020
Reglas AWS administradas actualizadas para AWS WAF	AWS Reglas administradas para AWS WAF actualizar los grupos de WordPress aplicaciones y `AWSManagedRulesCommonRuleSet` reglas.	3 de marzo de 2020
Se agregó el chequeo de estado de Amazon Route 53 a las opciones AWS Shield Advanced de protección	Shield Advanced ahora admite el uso de asociaciones de comprobación de estado de Amazon Route 53 para mejorar la precisión de la detección y mitigación de amenazas.	14 de febrero de 2020

Se actualizaron las reglas AWS administradas para AWS WAF	AWS Managed Rules for AWS WAF ha actualizado el grupo de reglas de la base de datos SQL para añadir la comprobación del URI del mensaje.	23 de enero de 2020
Nueva opción de Firewall Manager de política de auditoría de uso del grupo de seguridad	Firewall Manager tiene una nueva opción de políticas de auditoría de uso del grupo de seguridad. Ahora puede establecer un número mínimo de mínimo que un grupo de seguridad debe permanecer sin uso antes de que se considere no conforme. De forma predeterminada, esta configuración de minutos es cero.	14 de enero de 2020
Firewall Manager: nueva opción para la AWS WAF política	Firewall Manager tiene una nueva opción para AWS WAF las políticas. Ahora puede elegir eliminar todas las asociaciones ACL web existentes de los recursos dentro del ámbito antes de asociar las nuevas ACL web de la política.	14 de enero de 2020
Reglas AWS administradas actualizadas para AWS WAF	AWS Managed Rules for AWS WAF ha actualizado las transformaciones de texto de las reglas del conjunto de reglas principales y de los grupos de reglas de la base de datos SQL.	20 de diciembre de 2019

AWS Firewall Manager integrado con AWS Security Hub	AWS Firewall Manager ahora detecta los recursos que no cumplen con las normas y los ataques y los envía a AWS Security Hub.	18 de diciembre de 2019

Publicación de la AWS WAF versión 2	Nueva versión de la guía para AWS WAF desarroll adores. Puede administrar una ACL web o un grupo de reglas en formato JSON. Las capacidades ampliadas incluyen instrucciones de reglas lógicas, anidamiento de instrucciones de reglas y compatibilidad completa con CIDR para direcciones IP y rangos de direcciones. Las reglas ya no son AWS recursos, sino que solo existen en el contexto de una ACL web o un grupo de reglas. Para los clientes actuales, la versión anterior del servicio ahora se denomina AWS WAF Classic. En las API, los SDK y las CLI, AWS WAF Classic conserva sus esquemas de nomenclatura y AWS WAF se hace referencia a esta última versión con la adición de «V2" o «v2", según el contexto. AWS WAF no puede acceder a AWS los recursos que se crearon en Classic. AWS WAF Para utilizar esos recursos AWS WAF, debe migrarlos.	25 de noviembre de 2019
AWS Grupos de reglas de Managed Rules para AWS WAF	Se agregaron grupos de reglas de reglas AWS administradas. Son gratuitos para AWS WAF los clientes.	25 de noviembre de 2019

AWS Firewall Manager soporte para grupos de seguridad de Amazon Virtual Private Cloud	Se ha agregado compatibilidad con grupos de seguridad de Amazon VPC a Firewall Manager.	10 de octubre de 2019
AWS Firewall Manager soporte para AWS Shield Advanced	Se ha agregado compatibilidad con Shield Advanced a Firewall Manager.	15 de marzo de 2019
Tutorial: Crear políticas jerárquicas	Se ha añadido un tutorial sobre la creación de políticas jerárquicas en AWS Firewall Manager.	11 de febrero de 2019
Control en el nivel de regla en grupos de reglas	Ahora puede excluir reglas individuales de los grupos de AWS Marketplace reglas, así como sus propios grupos de reglas.	12 de diciembre de 2018
AWS Shield Advanced soporte para aceleradores AWS Global Accelerator estándar	Shield Advanced ahora puede proteger los aceleradores AWS Global Accelerator estándar.	26 de noviembre de 2018
AWS WAF compatibilidad con Amazon API Gateway	AWS WAF ahora protege las API de Amazon API Gateway.	25 de octubre de 2018
Asistente de inicio avanzado de Expanded AWS Shield	El nuevo asistente brinda la oportunidad de crear reglas basadas en tarifas y Amazon CloudWatch Events.	31 de agosto de 2018
AWS WAF registro	Habilite el registro para obtener información detallada sobre el tráfico que analiza su ACL web.	31 de agosto de 2018

Compatibilidad con los parámetros de consulta en las condiciones	Al crear una condición, ahora puede buscar en las solicitud es parámetros específicos.	5 de junio de 2018
Asistente de introducción a Shield Advanced	Introduce un nuevo proceso simplificado para suscribirse a AWS Shield Advanced.	5 de junio de 2018
Intervalos de CIDR permitidos ampliados	Al crear una condición de coincidencia de IP, AWS WAF ahora es compatible con los rangos de direcciones IPv4: /8 y cualquier rango entre /16 y /32.	5 de junio de 2018

Actualizaciones antes de 2018

En la siguiente tabla se describen los cambios importantes que se han realizado en cada una de las versiones de la Guía para desarrolladores de AWS WAF anteriores a 2018.

Cambio	Versión de API	Descripción	Fecha de lanzamien to
Actualiza ción	24/08/2016	AWS Marketplace grupos de reglas	Noviembre de 2017
Actualiza ción	24/08/2016	Compatibilidad de Shield Advanced con direcciones IP elásticas	Noviembre de 2017
Actualiza ción	24/08/2016	Panel de amenazas globales	Noviembre de 2017
Actualiza ción	24/08/2016	Tutorial sobre sitios web resistentes a ataques DDoS	Octubre de 2017

Cambio	Versión de API	Descripción	Fecha de lanzamiento
Actualización	24/08/2016	Condiciones geográficas y regex	Octubre de 2017
Actualización	24/08/2016	Reglas basadas en frecuencia	Junio de 2017
Actualización	24/08/2016	Reorganización	Abril de 2017
Actualización	24/08/2016	Información añadida sobre protección DDOS y soporte para Application Load Balancers.	Noviembre de 2016
Nuevas características	24/08/2015	Ahora puede registrar todas sus llamadas a la API en AWS WAF through AWS CloudTrail, el AWS servicio que registra las llamadas a la API de su cuenta y entrega los archivos de registro a su bucket de S3. CloudTrail Los registros se pueden utilizar para realizar análisis de seguridad, realizar un seguimiento de los cambios en sus AWS recursos y facilitar la auditoría de conformidad. La integración AWS WAF CloudTrail permite determinar qué solicitudes se han realizado a la AWS WAF API, la dirección IP de origen desde la que se ha realizado cada solicitud, quién ha realizado la solicitud, cuándo se ha realizado, etc. Si ya la utilizas AWS CloudTrail, empezarás a ver las llamadas a la AWS WAF API en tu CloudTrail registro. Si no la has activado CloudTrail en tu cuenta, puedes activarla CloudTrail desde AWS Management Console. La activación no conlleva ningún cargo adicional CloudTrail, pero se aplican las tarifas estándar por el uso de Amazon S3 y Amazon SNS.	28 de abril de 2016

Cambio	Versión de API	Descripción	Fecha de lanzamiento
Nuevas características	24/08/2015	Ahora puede utilizarlas AWS WAF para permitir, bloquear o contar las solicitudes web que parezcan contener scripts maliciosos, lo que se conoce como secuencias de comandos entre sitios o XSS. Los atacantes a veces insertan scripts maliciosos en solicitudes web para aprovechar las vulnerabilidades de las aplicaciones web. Para obtener más información, consulte Instrucción de regla de ataques de scripting entre sitios.	29 de marzo de 2016
Nuevas características	24/08/2015	Con esta versión, AWS WAF añade las siguientes funciones: • Puede configurarlo AWS WAF para permitir, bloquear o contar las solicitudes web en función de la longitud de las partes especificadas de las solicitudes, como las cadenas de consulta o los URI. Para obtener más información, consulte Instrucción de regla de restricción de tamaño. • Puedes configurarlo AWS WAF para permitir, bloquear o contar las solicitudes web en función del contenido del cuerpo de la solicitud. Esta es la parte de una solicitud que contiene los datos adicionales que desea enviar a su servidor web como el cuerpo de la solicitud HTTP, por ejemplo, los datos de un formulario. Esta característica se aplica a condiciones de coincidencia de cadenas, de coincidencia de inyección de código SQL y las nuevas condiciones de limitación de tamaño mencionados en el primer punto. Para obtener más información, consulte Especificación y manejo de componentes de solicitudes web.	27 de enero de 2016

Cambio	Versión de API	Descripción	Fecha de lanzamiento
Nueva característica	24/08/2015	Ahora puede usar la AWS WAF consola para elegir las CloudFront distribuciones a las que desea asociar una ACL web. Para obtener más información, consulte Asociar o desasociar una ACL web y una distribución. CloudFront	16 de noviembre de 2015
Versión inicial	24/08/2015	Esta es la primera versión de la Guía para desarrolladores de AWS WAF .	6 de octubre de 2015

AWS Glosario

Para obtener la AWS terminología más reciente, consulte el AWS glosario de la Glosario de AWS Referencia.

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.