Guida per gli sviluppatori

AWS WAFAWS Firewall Manager, e AWS Shield Advanced

AWS WAFAWS Firewall Manager, e AWS Shield Advanced: Guida per gli sviluppatori

Table of Contents

Cosa sono AWS WAF, AWS Shield e AWS Firewall Manager?

È possibile utilizzare AWS WAF e creare AWS Firewall Manager insieme una soluzione di sicurezza completa. AWS Shield AWS WAF è un firewall per applicazioni Web che è possibile utilizzare per monitorare le richieste Web inviate dagli utenti finali alle applicazioni e per controllare l'accesso ai contenuti. AWS Shield fornisce protezione contro gli attacchi DDoS (Distributed Denial of Service) alle AWS risorse, a livello di rete e trasporto (livelli 3 e 4) e a livello di applicazione (livello 7). AWS Firewall Manager fornisce la gestione di protezioni come AWS WAF Shield Advanced tra account e risorse, anche quando vengono aggiunte nuove risorse.

Argomenti

- AWS WAF
- AWS Shield
- AWS Firewall Manager

AWS WAF

AWS WAF è un firewall per applicazioni Web che consente di monitorare le richieste HTTP e HTTPS inoltrate alle risorse protette delle applicazioni Web. È possibile proteggere i seguenti tipi di risorse:

- CloudFront Distribuzione Amazon
- API REST di Amazon API Gateway
- Application Load Balancer
- AWS AppSync API GraphQL
- Bacino d'utenza di Amazon Cognito
- AWS App Runner servizio
- AWS istanza Verified Access

AWS WAF ti consente di controllare l'accesso ai tuoi contenuti. In base alle condizioni specificate, come gli indirizzi IP da cui provengono le richieste o i valori delle stringhe di query, la risorsa protetta risponde alle richieste con il contenuto richiesto, con un codice di stato HTTP 403 (Proibito) o con una risposta personalizzata.

Al livello più semplice, AWS WAF consente di scegliere uno dei seguenti comportamenti:

- Consenti tutte le richieste tranne quelle specificate: è utile quando desideri che Amazon CloudFront, Amazon API Gateway, Application Load Balancer AWS AppSync, Amazon Cognito AWS App Runner AWS o Verified Access forniscano contenuti per un sito Web pubblico, ma desideri anche bloccare le richieste degli aggressori.
- Blocca tutte le richieste tranne quelle specificate: è utile quando desideri fornire contenuti per un sito Web con restrizioni i cui utenti sono facilmente identificabili dalle proprietà nelle richieste Web, come gli indirizzi IP che utilizzano per accedere al sito Web.
- Conta le richieste che soddisfano i tuoi criteri: puoi utilizzare l'Countazione per tracciare il traffico web senza modificare il modo in cui lo gestisci. Puoi utilizzarla per il monitoraggio generale e anche per testare le tue nuove regole di gestione delle richieste web. Quando desideri consentire o bloccare le richieste basate su nuove proprietà nelle richieste Web, puoi prima configurare il conteggio delle richieste che corrispondono AWS WAF a tali proprietà. Ciò consente di confermare le nuove impostazioni di configurazione prima di modificare le regole per consentire o bloccare le richieste corrispondenti.
- Esegui controlli CAPTCHA o contestazioni su richieste che soddisfano i tuoi criteri: puoi implementare i controlli CAPTCHA e le contestazioni silenziose contro le richieste per ridurre il traffico dei bot verso le tue risorse protette.

L'utilizzo offre diversi vantaggi AWS WAF :

- Protezione aggiuntiva contro gli attacchi Web utilizzando criteri specificati dall'utente. È possibile definire criteri utilizzando caratteristiche delle richieste Web come le seguenti:
  - Gli indirizzi IP di origine delle richieste.
  - Il paese di origine delle richieste.
  - I valori nelle intestazioni della richiesta.
  - Stringhe che appaiono nelle richieste, stringhe specifiche o stringhe che corrispondono a modelli di espressioni regolari (regex).
  - Lunghezza delle richieste.
  - Presenza di codice SQL che può essere dannoso (noto come SQL injection).
  - Presenza di uno script che potrebbe essere dannoso (noto come Cross-site scripting).
- Regole in grado di consentire, bloccare o contare le richieste Web che soddisfano i criteri specificati. In alternativa, le regole possono bloccare o contare le richieste Web che non solo

soddisfano i criteri specificati, ma superano anche un determinato numero di richieste in un minuto o in cinque minuti.

- Regole che è possibile riutilizzare per più applicazioni Web.
- Gruppi di regole gestiti da AWS e Marketplace AWS venditori.
- Metriche in tempo reale e richieste Web campionate.
- Amministrazione automatizzata tramite l' AWS WAF API.

Se desideri un controllo granulare sulle protezioni che aggiungi alle tue risorse, AWS WAF da sola potrebbe essere la scelta giusta. Per ulteriori informazioni su AWS WAF, consulta. AWS WAF

AWS Shield

È possibile utilizzare AWS WAF elenchi di controllo degli accessi Web (Web ACL) per ridurre al minimo gli effetti di un attacco DDoS (Distributed Denial of Service). Per una protezione aggiuntiva contro gli attacchi DDoS, AWS fornisce anche e. AWS Shield Standard AWS Shield Advanced AWS Shield Standard è incluso automaticamente senza costi aggiuntivi oltre a quelli già pagati AWS WAF e agli altri AWS servizi.

AWS Shield Advanced offre una protezione estesa dagli attacchi DDoS per le istanze Amazon EC2, i sistemi di bilanciamento del carico Elastic Load Balancing, le distribuzioni CloudFront , le zone ospitate Route 53 e gli acceleratori standard. AWS Global Accelerator AWS Shield Advanced comporta costi aggiuntivi. Le opzioni e le funzionalità di Shield Advanced includono la mitigazione automatica degli attacchi DDoS a livello di applicazione, la visibilità avanzata degli eventi e il supporto dedicato dello Shield Response Team (SRT). Se possiedi siti Web ad alta visibilità o sei comunque soggetto a frequenti attacchi DDoS, valuta la possibilità di acquistare le protezioni aggiuntive fornite da Shield Advanced. Per ulteriori informazioni, consulta AWS Shield Advanced funzionalità e opzioni e Decidere se abbonarsi AWS Shield Advanced e applicare protezioni aggiuntive.

AWS Firewall Manager

AWS Firewall Manager semplifica le attività di amministrazione e manutenzione su più account e risorse per una varietà di protezioni AWS WAF, tra cui gruppi di sicurezza AWS Shield Advanced Amazon VPC AWS Network Firewall e Amazon Route 53 Resolver DNS Firewall. Con Firewall Manager, configuri le protezioni una sola volta e il servizio le applica automaticamente a tutti i tuoi account e risorse, anche quando aggiungi nuovi account e risorse.

Per ulteriori informazioni su Firewall Manager, consulta AWS Firewall Manager.

Configurazione

In questo argomento vengono descritti i passaggi preliminari, come la creazione di un account, per prepararsi all'uso di AWS WAF AWS Firewall Manager, e AWS Shield Advanced. Questi articoli preliminari non ti vengono addebitati. Ti vengono addebitati solo i AWS servizi che utilizzi.

Argomenti

Iscriviti per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Creazione di un utente amministratore

Dopo la registrazione Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Creazione di un utente amministratore

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In Centro identità AWS IAM, assegna l'accesso amministrativo a un utente amministrativo.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Download degli strumenti

AWS Management Console Include una console per AWS WAF, e AWS Shield Advanced AWS Firewall Manager, ma se desideri accedere ai servizi a livello di codice, consulta quanto segue:

- Le guide alle API documentano le operazioni supportate dai servizi e forniscono collegamenti alla documentazione SDK e CLI correlata:
  - AWS WAF Documentazione di riferimento delle API
  - AWS Shield Advanced Documentazione di riferimento delle API
  - AWS Firewall Manager Documentazione di riferimento delle API
- Per chiamare un'API senza dover gestire dettagli di basso livello come l'assemblaggio di richieste HTTP non elaborate, puoi utilizzare un SDK. AWS Gli AWS SDK forniscono funzioni e tipi di dati che incapsulano la funzionalità dei servizi. AWS Per scaricare un AWS SDK e accedere alle istruzioni di installazione, consulta la pagina pertinente:
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  Per un elenco completo degli AWS SDK, consulta Tools for Amazon Web Services.
- Puoi usare il AWS Command Line Interface (AWS CLI) per controllare più AWS servizi dalla riga di comando. È inoltre possibile automatizzare i comandi utilizzando gli script. Per ulteriori informazioni, consulta AWS Command Line Interface.
- AWS Tools for Windows PowerShell supporta questi AWS servizi. Per ulteriori informazioni, consulta la Documentazione di riferimento per Cmdlet AWS Tools for PowerShell.

AWS WAF

AWS WAF è un firewall per applicazioni Web che consente di monitorare le richieste HTTP (S) inoltrate alle risorse protette delle applicazioni Web. È possibile proteggere i seguenti tipi di risorse:

- CloudFront Distribuzione Amazon
- API REST di Amazon API Gateway
- Application Load Balancer
- AWS AppSync API GraphQL
- Bacino d'utenza di Amazon Cognito
- AWS App Runner servizio
- AWS istanza Verified Access

AWS WAF ti consente di controllare l'accesso ai tuoi contenuti. In base a criteri specificati dall'utente, ad esempio gli indirizzi IP da cui provengono le richieste o i valori delle stringhe di query, il servizio associato alla risorsa protetta risponde alle richieste con il contenuto richiesto, con un codice di stato HTTP 403 (Proibito) o con una risposta personalizzata.

> **Note**
>
> Puoi anche utilizzarle AWS WAF per proteggere le tue applicazioni ospitate in contenitori Amazon Elastic Container Service (Amazon ECS). Amazon ECS è un servizio di gestione dei container veloce e altamente scalabile che semplifica l'esecuzione, l'arresto e la gestione dei contenitori Docker su un cluster. Per utilizzare questa opzione, configuri Amazon ECS per utilizzare un Application Load Balancer abilitato AWS WAF per instradare e proteggere il traffico HTTP (S) layer 7 tra le attività del tuo servizio. Per ulteriori informazioni, consulta Service Load Balancing nella Amazon Elastic Container Service Developer Guide.

Argomenti

- AWS WAF regole
- Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF
- Corrispondenza dei modelli di espressioni regolari in AWS WAF
- Set IP e set di pattern regex in AWS WAF
- Richieste e risposte web personalizzate in AWS WAF
- AWS WAF etichette sulle richieste web
- AWS WAF mitigazione intelligente delle minacce
- Registrazione del traffico AWS WAF ACL Web
- Test e ottimizzazione delle protezioni AWS WAF
- Come AWS WAF funziona con le CloudFront funzionalità di Amazon
- Sicurezza nell'utilizzo del AWS WAF servizio
- AWS WAF quote
- Migrazione delle risorse AWS WAF Classic a AWS WAF

Come AWS WAF funziona

Lo usi AWS WAF per controllare il modo in cui le tue risorse protette rispondono alle richieste web HTTP (S). A tale scopo, è necessario definire una lista di controllo degli accessi Web (ACL) e quindi associarla a una o più risorse dell'applicazione Web che si desidera proteggere. Le risorse associate inoltrano le richieste in arrivo all' AWS WAF ACL Web per l'ispezione.

Nell'ACL Web, crei regole per definire i modelli di traffico da cercare nelle richieste e per specificare le azioni da intraprendere in caso di richieste corrispondenti. Le scelte di azione includono quanto segue:

- Consenti alle richieste di passare alla risorsa protetta per l'elaborazione e la risposta.
- Blocca le richieste.
- Conta le richieste.
- Esegui controlli CAPTCHA o contesta le richieste per verificare l'utilizzo standard del browser da parte degli utenti umani.

AWS WAF componenti

Di seguito sono riportati i componenti principali di AWS WAF:

- ACL Web: si utilizza una lista di controllo degli accessi Web (ACL) per proteggere un set di AWS risorse. È possibile creare un'ACL Web e definire la sua strategia di protezione aggiungendo regole. Le regole definiscono i criteri per l'ispezione delle richieste Web e specificano l'azione da intraprendere sulle richieste che soddisfano i criteri specificati. È inoltre possibile impostare un'azione predefinita per l'ACL Web che indica se bloccare o consentire l'invio di tutte le richieste che le regole non hanno già bloccato o consentito. Per ulteriori informazioni sulle ACL Web, consulta Elenchi di controllo degli accessi Web (ACL Web).

  Un ACL web è una AWS WAF risorsa.
- Regole: ogni regola contiene un'istruzione che definisce i criteri di ispezione e un'azione da intraprendere se una richiesta Web soddisfa i criteri. Quando una richiesta Web soddisfa i criteri, questa è una corrispondenza. Puoi configurare regole per bloccare le richieste corrispondenti, consentirle di passare, contarle o eseguire controlli bot su di esse utilizzando puzzle CAPTCHA o sfide silenziose del browser client. Per ulteriori informazioni sulle regole, consulta AWS WAF regole.

  Una regola non è una risorsa. AWS WAF Esiste solo nel contesto di un ACL Web o di un gruppo di regole.
- Gruppi di regole: è possibile definire le regole direttamente all'interno di un ACL Web o in gruppi di regole riutilizzabili. AWS Managed Rules e Marketplace AWS i venditori forniscono gruppi di regole gestiti da utilizzare. Puoi anche definire i tuoi gruppi di regole. Per ulteriori informazioni sui gruppi di regole, consulta Gruppi di regole.

  Un gruppo di regole è una AWS WAF risorsa.

Argomenti

AWS WAF unità di capacità Web ACL (WCU)

AWS WAF utilizza le unità di capacità Web ACL (WCU) per calcolare e controllare le risorse operative necessarie per eseguire le regole, i gruppi di regole e gli ACL Web. AWS WAF applica i limiti WCU quando configuri i gruppi di regole e gli ACL web. Le WCU non influiscono sul modo in cui ispeziona il traffico web. AWS WAF

AWS WAF gestisce la capacità per regole, gruppi di regole e ACL Web.

Regola WCU

AWS WAF calcola la capacità delle regole quando si crea o si aggiorna una regola. AWS WAF calcola la capacità in modo diverso per ogni tipo di regola, per riflettere il costo relativo di ogni regola. Regole semplici la cui esecuzione costa poco utilizzano un numero inferiore di WCU rispetto a regole più complesse che utilizzano più potenza di elaborazione. Ad esempio, un'istruzione su una regola di vincolo di dimensione utilizza meno WCU rispetto a un'istruzione che esamina le richieste utilizzando un set di pattern regex.

I requisiti di capacità delle regole generalmente partono da un costo base per il tipo di regola e aumentano con la complessità, ad esempio quando si aggiungono trasformazioni di testo prima dell'ispezione o se si ispeziona il corpo JSON. Per informazioni sui requisiti di capacità delle regole, consulta gli elenchi delle istruzioni delle regole all'indirizzo. Nozioni di base sulla dichiarazione delle regole

Gruppo di regole WCU

I requisiti WCU per un gruppo di regole sono determinati dalle regole definite all'interno del gruppo di regole. La capacità massima per un gruppo di regole è di 5.000 WCU.

Ogni gruppo di regole ha un'impostazione di capacità immutabile, che il proprietario assegna al momento della creazione. Questo vale per i gruppi di regole gestiti e i gruppi di regole mediante i quali si creano. AWS WAF Quando si modifica un gruppo di regole, le modifiche devono mantenere le WCU del gruppo di regole entro i limiti della sua capacità. Ciò garantisce che gli ACL Web che utilizzano il gruppo di regole rimangano entro i requisiti di capacità.

Le WCU utilizzate in un gruppo di regole sono la somma delle WCU per le regole meno le ottimizzazioni di elaborazione ottenibili combinando il comportamento delle regole. AWS WAF Ad esempio, se definisci due regole per esaminare lo stesso componente di richiesta web e ciascuna di esse applica una particolare trasformazione al componente prima di esaminarlo, AWS WAF potresti essere in grado di addebitarti una sola volta per l'applicazione della trasformazione. Il costo WCU per l'utilizzo di un gruppo di regole in un ACL Web è sempre l'impostazione WCU fissa definita al momento della creazione del gruppo di regole.

Quando crei un gruppo di regole, fai attenzione a impostare la capacità sufficientemente alta da soddisfare le regole che desideri utilizzare per tutta la durata del gruppo di regole.

WCU Web ACL

I requisiti WCU per un ACL Web sono determinati dalle regole e dai gruppi di regole utilizzati all'interno dell'ACL Web.

- Il costo dell'utilizzo di un gruppo di regole in un ACL Web è l'impostazione della capacità del gruppo di regole.
- Il costo dell'utilizzo di una regola è dato dalle WCU calcolate dalla regola meno le ottimizzazioni di elaborazione ottenibili dalla combinazione di regole dell'ACL Web. AWS WAF Ad esempio, se definisci due regole per esaminare lo stesso componente di richiesta web e ciascuna di esse applica una particolare trasformazione al componente prima di esaminarlo, AWS WAF potresti essere in grado di addebitarti una sola volta per l'applicazione della trasformazione.

Il prezzo base di un ACL web include fino a 1.500 WCU. L'utilizzo di più di 1.500 WCU comporta costi aggiuntivi, secondo un modello di prezzo a più livelli. AWS WAF regola automaticamente i prezzi Web ACL al variare dell'utilizzo della WCU Web ACL. Per i dettagli sui prezzi, vedere Prezzi di AWS WAF.

La capacità massima per un ACL Web è di 5.000 WCU.

Determinazione dell'utilizzo della WCU

Come indicato nelle sezioni precedenti, le WCU totali utilizzate in un gruppo di regole o ACL web saranno uguali o inferiori alla somma delle WCU per tutte le regole definite nel gruppo di regole o nell'ACL web.

Nella AWS WAF console, è possibile visualizzare la capacità consumata quando si aggiungono regole all'ACL Web o al gruppo di regole. La console mostra le unità di capacità correnti utilizzate durante l'aggiunta delle regole.

Tramite l'API, è possibile verificare i requisiti di capacità massima per le regole che si desidera utilizzare in un ACL Web o in un gruppo di regole. A tale scopo, fornisci l'elenco JSON delle regole alla chiamata check capacity. Per ulteriori informazioni, consulta la pagina CheckCapacitydi riferimento dell'API AWS WAF V2.

Risorse con cui puoi proteggerti AWS WAF

È possibile utilizzare un ACL AWS WAF Web per proteggere i tipi di risorse globali o regionali. A tale scopo, è necessario associare l'ACL Web alle risorse che si desidera proteggere. L'ACL Web e tutte AWS WAF le risorse che utilizza devono trovarsi nella regione in cui si trova la risorsa associata. Per CloudFront le distribuzioni Amazon, questo valore è impostato su Stati Uniti orientali (Virginia settentrionale).

CloudFront Distribuzioni Amazon

Puoi associare un ACL AWS WAF Web a una CloudFront distribuzione utilizzando la AWS WAF console o le API. È inoltre possibile associare un ACL Web a una CloudFront distribuzione quando si crea o si aggiorna la distribuzione stessa. Per configurare un'associazione in AWS CloudFormation, è necessario utilizzare la configurazione di CloudFront distribuzione. Per informazioni su Amazon CloudFront, consulta Using AWS WAF to Control Access to Your Content nella Amazon CloudFront Developer Guide.

AWS WAF è disponibile a livello globale per CloudFront le distribuzioni, ma è necessario utilizzare la regione Stati Uniti orientali (Virginia settentrionale) per creare l'ACL Web e tutte le risorse utilizzate nell'ACL Web, come gruppi di regole, set IP e set di pattern regex. Alcune interfacce offrono la scelta della regione «Global ()». CloudFront La scelta di questa opzione è identica alla scelta della regione Stati Uniti orientali (Virginia settentrionale) o "»us-east-1.

Risorse regionali

Puoi proteggere le risorse regionali in tutte le regioni in cui AWS WAF è disponibile. È possibile visualizzare l'elenco negli AWS WAF endpoint e nelle quote in. Riferimenti generali di Amazon Web Services

È possibile utilizzare AWS WAF per proteggere i seguenti tipi di risorse regionali:

- API REST di Amazon API Gateway
- Application Load Balancer
- AWS AppSync API GraphQL
- Bacino d'utenza di Amazon Cognito
- AWS App Runner servizio
- AWS istanza Verified Access

È possibile associare un ACL Web solo a un Application Load Balancer che si trova all'interno. Regioni AWS Ad esempio, non è possibile associare un ACL Web a un Application Load Balancer attivo. AWS Outposts

L'ACL Web e tutte AWS WAF le altre risorse che utilizza devono trovarsi nella stessa regione delle risorse protette. Durante il monitoraggio e la gestione delle richieste Web per una risorsa regionale protetta, AWS WAF mantiene tutti i dati nella stessa regione della risorsa protetta.

Restrizioni sulle associazioni di più risorse

È possibile associare un singolo ACL Web a una o più AWS risorse, con le seguenti restrizioni:

- È possibile associare ogni AWS risorsa a un solo ACL web. La relazione tra l'ACL web e AWS le risorse è. one-to-many
- È possibile associare un ACL Web a una o più CloudFront distribuzioni. Non è possibile associare un ACL Web associato a una CloudFront distribuzione a nessun altro AWS tipo di risorsa.

Iniziare con AWS WAF

Questo tutorial mostra come utilizzare AWS WAF per eseguire le seguenti attività:

- Configurare AWS WAF.
- Crea un elenco di controllo degli accessi Web (Web ACL) utilizzando la procedura guidata nella AWS WAF console.
- Scegli le AWS risorse per le quali desideri AWS WAF esaminare le richieste web. Questo tutorial illustra i passaggi per Amazon CloudFront. Il processo è essenzialmente lo stesso per un'API REST di Amazon API Gateway, un Application Load Balancer, un'API GraphQL AWS AppSync , un pool di utenti Amazon Cognito, un AWS App Runner servizio o un'istanza Verified Access. AWS
- Aggiungere le regole e i gruppi di regole che si desidera utilizzare per filtrare le richieste Web. Ad esempio, puoi specificare gli indirizzi IP da cui provengono le richieste e specificare i valori nella richiesta che vengono utilizzati solo dagli aggressori. Per ogni regola, si specifica come gestire le richieste Web corrispondenti. Puoi fare cose come bloccarle o contarle e puoi eseguire sfide bot come CAPTCHA. Definisci un'azione per ogni regola che definisci all'interno di un ACL web e per ogni regola che definisci all'interno di un gruppo di regole.
- Specificate un'azione predefinita per l'ACL Web, oppureBlock. Allow Questa è l'azione che viene AWS WAF eseguita su una richiesta quando le regole dell'ACL Web non la consentono o la bloccano esplicitamente.

> **Note**
>
> AWS in genere ti addebita meno di 0,25 USD al giorno per le risorse che crei durante questo tutorial. Una volta completato il tutorial, ti consigliamo di eliminare le risorse per evitare di incorrere in spese non necessarie.

Argomenti

Fase 1: Configurazione AWS WAF

Se non hai già seguito la procedura di configurazione generale riportata in precedenzaConfigurazione, fallo ora.

Fase 2: creare un'ACL Web

La AWS WAF console guida l'utente attraverso il processo di configurazione AWS WAF per bloccare o consentire le richieste Web in base a criteri specificati dall'utente, ad esempio gli indirizzi IP da cui provengono le richieste o i valori nelle richieste. In questa fase verrà creata un'ACL Web. Per ulteriori informazioni sugli ACL AWS WAF Web, vedere. Elenchi di controllo degli accessi Web (ACL Web)

Per creare un'ACL Web

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Dalla AWS WAF home page, scegli Crea ACL web.
3. Per Name (Nome), immettere il nome che si desidera utilizzare per identificare l'ACL Web.

   > **Note**
   >
   > Non è possibile modificare il nome dopo aver creato l'ACL Web.

4. (Facoltativo) Per Description - optional (Descrizione - facoltativo), immettere una descrizione più lunga per l'ACL Web, se richiesta.
5. Per il nome della CloudWatch metrica, modifica il nome predefinito, se applicabile. Seguire le linee guida sulla console per i caratteri validi. Il nome non può contenere caratteri speciali, spazi vuoti o nomi parametro riservati per AWS WAF, inclusi "All" e "Default_Action".

> **Note**
>
> Non è possibile modificare il nome della CloudWatch metrica dopo aver creato l'ACL Web.

6. Per Tipo di risorsa, scegli CloudFront le distribuzioni. La regione viene compilata automaticamente in Global (CloudFront) per CloudFront le distribuzioni.
7. (Facoltativo) Per AWS Risorse associate: facoltativo, scegli Aggiungi AWS risorse. Nella finestra di dialogo, scegli le risorse che desideri associare, quindi scegli Aggiungi. AWS WAF torna alla pagina Descrivi web ACL e AWS risorse associate.
8. Seleziona Successivo.

Fase 3: aggiungere una regola di corrispondenza stringa

In questa fase, viene creata una regola con un'istruzione di corrispondenza stringa e indicato cosa fare con le richieste corrispondenti. Un'istruzione String Match Rule identifica le stringhe che si desidera AWS WAF cercare in una richiesta. Di solito, una stringa è composta da caratteri ASCII stampabili, ma è possibile specificare qualsiasi carattere esadecimale da 0x00 a 0xFF (decimale da 0 a 255). Oltre a specificare la stringa da cercare, specificate il componente della richiesta Web in cui desiderate cercare, ad esempio un'intestazione, una stringa di query o il corpo della richiesta.

Questo tipo di istruzione funziona su un componente di richiesta Web e richiede le seguenti impostazioni del componente di richiesta:

- Componente di richiesta: la parte della richiesta Web per ispezionare, ad esempio, una stringa di query o il corpo.

> **Warning**
>
> Se ispezionate i componenti della richiesta Body, JSON body, Headers o Cookies, leggete le limitazioni relative alla quantità di contenuto AWS WAF che può essere ispezionata. Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF

Per informazioni sui componenti della richiesta Web, consulta. Componenti delle richieste Web

- Trasformazioni di testo opzionali: trasformazioni che si desidera AWS WAF eseguire sul componente della richiesta prima di esaminarlo. Ad esempio, potete trasformare in lettere minuscole o normalizzare lo spazio bianco. Se specificate più di una trasformazione, le AWS WAF elabora nell'ordine elencato. Per informazioni, consulta Trasformazioni di testo.

Per ulteriori informazioni sulle AWS WAF regole, vedereAWS WAF regole.

Per creare un'istruzione regola di corrispondenza stringa

1. Nella pagina Add rules and rule groups (Aggiungi regole e gruppi di regole), scegliere Add rules (Aggiungi regole), Add my own rules and rule groups (Aggiungi le mie regole e i miei gruppi di regole), Rule builder (Generatore di regole), quindi Rule visual editor (Editor visivo delle regole).

   > **Note**
   >
   > La console fornisce Rule visual editor (Editor visivo delle regole) e anche un Rule JSON editor (Editor JSON delle regole). L'editor JSON semplifica l'operazione di copia delle configurazioni tra ACL Web ed è necessario per set di regole più complesse, come quelle con più livelli di nidificazione.
   > Questa procedura utilizza Rule visual editor (Editor visivo delle regole).

2. In Name (Nome), immettere il nome che si desidera utilizzare per identificare questa regola.
3. In Type (Tipo), scegliere Regular rule (Regola normale).
4. In If a request (Se una richiesta), scegliere matches the statement (corrisponde all'istruzione).

   Le altre opzioni riguardano i tipi di istruzioni delle regole logiche. È possibile utilizzarle per combinare o annullare i risultati di altre istruzioni di regole.
5. In Statement, per Inspect, apri il menu a discesa e scegli il componente di richiesta web che desideri AWS WAF ispezionare. Per questo esempio, scegliere Header (Intestazione).

   Quando si sceglie Header (Intestazione), si specifica anche quale intestazione AWS WAF deve ispezionare. Specificare **`User-Agent`**. Questo valore non prevede la distinzione tra lettere maiuscole e minuscole.
6. Per Match type (Tipo di corrispondenza), scegliere la posizione in cui visualizzare la stringa specificata nell'intestazione `User-Agent`.

Per questo esempio, scegliere Exactly matches string (Corrispondenza stringa esatta). Ciò indica che AWS WAF ispeziona l'intestazione user-agent in ogni richiesta Web alla ricerca di una stringa identica alla stringa specificata.

7. In String to match (Stringa da abbinare), specificare una stringa che AWS WAF deve cercare. La lunghezza massima di String to match (Stringa da abbinare) è di 200 caratteri. Se si desidera specificare un valore con codifica base64, è possibile specificare fino a 200 caratteri prima della codifica.

   Per questo esempio, immettere. MyAgent AWS WAF esaminerà il valore nell'`User-Agent`intestazione delle richieste Web. `MyAgent`
8. Lasciare Text transformation (Trasformazione del testo) impostata su None (Nessuno).
9. In Azione, seleziona l'azione che desideri che la regola esegua quando corrisponde a una richiesta web. Per questo esempio, scegli Count e lascia le altre scelte invariate. L'azione Count crea metriche per le richieste Web che corrispondono alla regola, ma non influisce sul fatto che la richiesta sia consentita o bloccata. Per ulteriori informazioni sulle scelte di azione, consulta Operazione delle regole eValutazione delle regole ACL Web e dei gruppi di regole.
10. Scegli Aggiungi regola.

Passaggio 4: Aggiungere un gruppo di regole AWS gestite

AWS Managed Rules offre una serie di gruppi di regole gestiti da utilizzare, la maggior parte dei quali sono gratuiti per AWS WAF i clienti. Per ulteriori informazioni sui gruppi di regole, consulta Gruppi di regole. Aggiungeremo un gruppo di regole AWS Managed Rules a questo ACL web.

Per aggiungere un gruppo di regole AWS Managed Rules

1. Nella pagina Add rules and rule groups (Aggiungi regole e gruppi di regole), scegliere Add rules (Aggiungi regole), quindi Add managed rule groups (Aggiungi gruppi di regole gestite).
2. Nella pagina Add managed rule groups (Aggiungi gruppi di regole gestite), espandere l'elenco per i gruppi di regole gestite AWS . (Vedrai anche le inserzioni offerte ai Marketplace AWS venditori. Puoi iscriverti alle loro offerte e poi utilizzarle come per i gruppi di regole AWS Managed Rules.)
3. Per il gruppo di regole che desideri aggiungere, procedi come segue:

   a. Nella colonna Azione, attiva l'interruttore Aggiungi al web ACL.

b. Seleziona Modifica e, nell'elenco delle regole del gruppo di regole, apri il menu a discesa Sostituisci tutte le azioni delle regole e seleziona. Count Questa operazione consente di impostare l'operazione per tutte le regole nel gruppo di regole solo per contare. In questo modo puoi vedere come si comportano tutte le regole del gruppo di regole con le tue richieste web prima di utilizzarle.

c. Scegli Salva regola.

4. Nella pagina Aggiungi gruppi di regole gestiti, scegli Aggiungi regole. Verrà visualizzata nuovamente la pagina Aggiungi regole e gruppi di regole.

Passaggio 5: Completare la configurazione ACL Web

Al termine dell'aggiunta di regole e gruppi di regole alla configurazione dell'ACL Web, terminare gestendo la priorità delle regole nell'ACL Web e configurando impostazioni quali parametri, tagging e registrazione.

Per completare la configurazione dell'ACL Web

1. Nella pagina Add rules and rule groups (Aggiungi regole e gruppi di regole), scegliere Next (Avanti).
2. Nella pagina Imposta la priorità delle regole, puoi vedere l'ordine di elaborazione delle regole e dei gruppi di regole nell'ACL web. AWS WAF li elabora partendo dall'inizio dell'elenco. È possibile modificare l'ordine di elaborazione spostando le regole verso l'alto o verso il basso. A questo scopo, selezionarne uno nell'elenco e scegliere Move up (Sposta verso l'alto) o Move down (Sposta verso il basso). Per ulteriori informazioni sulla priorità delle regole, consulta Ordine di elaborazione delle regole e dei gruppi di regole in un ACL Web.
3. Seleziona Successivo.
4. Nella pagina Configura metriche, per i parametri di Amazon, puoi vedere i CloudWatch parametri pianificati per le tue regole e i tuoi gruppi di regole e puoi vedere le opzioni di campionamento delle richieste web. Per informazioni sulla visualizzazione delle richieste campionate, consulta. Visualizzazione di un esempio di richieste Web Per informazioni sui CloudWatch parametri di Amazon, consultaMonitoraggio con Amazon CloudWatch.

   Puoi accedere ai riepiloghi delle metriche del traffico web nella pagina Web ACL nella AWS WAF console, nella scheda Panoramica del traffico. Le dashboard della console forniscono riepiloghi quasi in tempo reale delle metriche Amazon del Web ACL. CloudWatch Per ulteriori informazioni, consulta la pagina Dashboard di panoramica sul traffico ACL Web.

5. Seleziona Next (Successivo).
6. Nella pagina Review and create web ACL (Rivedi e crea ACL Web), rivedere le impostazioni, quindi scegliere Create web ACL (Crea ACL Web).

La procedura guidata ripristina la visualizzazione della pagina Web ACL (Web ACL), dove viene elencata la nuova ACL Web.

Fase 6: eliminare le risorse

Il tutorial è stato completato con successo. Per evitare che sul tuo account vengano AWS WAF addebitati costi aggiuntivi, pulisci gli oggetti che hai creato. AWS WAF In alternativa, puoi modificare la configurazione in modo che corrisponda alle richieste Web che desideri effettivamente gestire utilizzando. AWS WAF

> **Note**
>
> AWS in genere ti addebita meno di 0,25 USD al giorno per le risorse che crei durante questo tutorial. Al termine, ti consigliamo di eliminare le risorse per evitare di incorrere in spese non necessarie.

Per eliminare gli oggetti per i quali viene addebitato un costo AWS WAF

1. Nella pagina Web ACL (Web ACL), selezionare l'ACL Web dall'elenco e scegliere Edit (Modifica).
2. Nella scheda AWS Risorse associate, per ogni risorsa associata, seleziona il pulsante di opzione accanto al nome della risorsa, quindi scegli Dissocia. Questo dissocia l'ACL web dalle tue risorse. AWS
3. In ciascuna delle schermate seguenti, scegliere Next (Avanti) fino a tornare alla pagina Web ACL (ACL Web) .

   Nella pagina Web ACL (ACL Web), selezionare l'ACL Web dall'elenco e scegliere Delete (Elimina).

Le regole e le dichiarazioni delle regole non esistono al di fuori del gruppo di regole e delle definizioni dell'ACL Web. Se elimini un'ACL Web, verranno eliminate tutte le regole individuali definite nell'ACL Web. Quando rimuovi un gruppo di regole da un'ACL Web, è sufficiente rimuovere il riferimento ad esso.

Elenchi di controllo degli accessi Web (ACL Web)

Un elenco di controllo degli accessi Web (Web ACL) offre un controllo granulare su tutte le richieste Web HTTP (S) a cui risponde la risorsa protetta. Puoi proteggere le risorse Amazon CloudFront, Amazon API Gateway, Application Load Balancer AWS AppSync, Amazon Cognito AWS e AWS App Runner Verified Access.

Puoi utilizzare criteri come quelli descritti di seguito per consentire o bloccare le richieste:

- Origine dell'indirizzo IP della richiesta
- Paese di origine della richiesta
- Corrispondenza stringa o corrispondenza espressione regolare (regex) in una parte della richiesta
- Dimensione di una parte particolare della richiesta
- Rilevamento di codice o script SQL dannoso

Puoi anche testare qualsiasi combinazione di queste condizioni. Puoi bloccare o contare le richieste web che non solo soddisfano le condizioni specificate, ma superano anche un determinato numero di richieste in un solo minuto. Puoi combinare le condizioni utilizzando operatori logici. Puoi anche eseguire puzzle CAPTCHA e sfidare sessioni client silenziose contro le richieste.

Indichi i criteri di abbinamento e le azioni da intraprendere sulle corrispondenze nelle AWS WAF istruzioni delle regole. È possibile definire le istruzioni delle regole direttamente all'interno dell'ACL Web e in gruppi di regole riutilizzabili utilizzati nell'ACL Web. Per un elenco completo delle opzioni, consulta e. Nozioni di base sulla dichiarazione delle regole Operazione delle regole

Per specificare i criteri di ispezione e gestione delle richieste Web, esegui le seguenti attività:

1. Scegliete l'azione Web ACL predefinitaBlock, Allow oppure, per le richieste Web che non corrispondono a nessuna delle regole specificate. Per ulteriori informazioni, consulta L'azione predefinita dell'ACL Web.
2. Aggiungi eventuali gruppi di regole che desideri utilizzare nell'ACL Web. I gruppi di regole gestite contengono in genere regole che bloccano le richieste Web. Per informazioni sui gruppi di regole, consulta Gruppi di regole.
3. Specificate criteri di corrispondenza aggiuntivi e istruzioni di gestione in una o più regole. Per aggiungere più di una regola, inizia con `AND` le `OR` nostre istruzioni e raccogli le regole che desideri combinare sotto di esse. Se desidera negare un'opzione della regola, nidifica la regola in un'istruzione NOT. Facoltativamente, puoi utilizzare una regola basata sulla frequenza anziché una

regola normale per limitare il numero di richieste provenienti da qualsiasi indirizzo IP che soddisfa le condizioni. Per ulteriori informazioni sulle regole, consulta AWS WAF regole.

Se aggiungi più di una regola a un ACL web, AWS WAF valuta le regole nell'ordine in cui sono elencate per l'ACL web. Per ulteriori informazioni, consulta Valutazione delle regole ACL Web e dei gruppi di regole.

Quando crei un'ACL Web, specifica i tipi di risorse con cui la vuoi utilizzare. Per informazioni, consulta Creazione di un'ACL Web. Dopo aver definito un'ACL Web, puoi associarla alle risorse per iniziare a proteggerle. Per ulteriori informazioni, consulta Associazione o dissociazione di un ACL Web con una risorsa AWS.

In che modo AWS le risorse gestiscono i ritardi di risposta da AWS WAF

In alcune occasioni, AWS WAF potrebbe verificarsi un errore interno che ritarda la risposta alle AWS risorse associate sull'opportunità di consentire o bloccare una richiesta. In tali occasioni, CloudFront in genere consente la richiesta o fornisce il contenuto, mentre i servizi regionali in genere negano la richiesta e non forniscono il contenuto.

Argomenti

- Valutazione delle regole ACL Web e dei gruppi di regole
- L'azione predefinita dell'ACL Web
- Gestione dei limiti di dimensione delle ispezioni corporee
- Configurazione del dominio CAPTCHA, challenge e token per un ACL web
- Utilizzo delle ACL Web

Valutazione delle regole ACL Web e dei gruppi di regole

Il modo in cui un'ACL Web gestisce una richiesta Web dipende da quanto segue:

- Le impostazioni di priorità numerica delle regole nell'ACL Web e all'interno dei gruppi di regole
- Le impostazioni dell'operazione sulle regole e l'ACL Web
- Eventuali modifiche apportate alle regole nei gruppi di regole aggiunti

Per un elenco delle impostazioni delle azioni delle regole, vedere. Operazione delle regole

È possibile personalizzare la gestione delle richieste e delle risposte nelle impostazioni delle regole e nelle impostazioni delle azioni ACL Web predefinite. Per informazioni, consulta Richieste e risposte web personalizzate in AWS WAF.

Argomenti

- Ordine di elaborazione delle regole e dei gruppi di regole in un ACL Web
- Come vengono gestite le azioni delle regole e dei gruppi di regole in un ACL Web
- Le azioni sostituiscono i gruppi di regole

Ordine di elaborazione delle regole e dei gruppi di regole in un ACL Web

In un ACL Web e all'interno di qualsiasi gruppo di regole, è possibile determinare l'ordine di valutazione delle regole utilizzando impostazioni di priorità numeriche. È necessario assegnare a ciascuna regola di un ACL Web un'impostazione di priorità univoca all'interno di tale ACL Web e assegnare a ogni regola di un gruppo di regole un'impostazione di priorità univoca all'interno di quel gruppo di regole.

> **Note**
>
> Quando gestisci gruppi di regole e ACL Web tramite la console, ti AWS WAF assegna impostazioni di priorità numeriche univoche in base all'ordine delle regole nell'elenco. AWS WAF assegna la priorità numerica più bassa alla regola nella parte superiore dell'elenco e la priorità numerica più alta alla regola in fondo.

Quando AWS WAF valuta un ACL Web o un gruppo di regole in base a una richiesta Web, valuta le regole dall'impostazione della priorità numerica più bassa fino a quando non trova una corrispondenza che interrompa la valutazione o esaurisce tutte le regole.

Ad esempio, supponiamo di avere le seguenti regole e gruppi di regole nell'ACL web, con priorità come mostrato:

- Regola 1: priorità 0
- RuleGroupA — priorità 100
  - Regola A1: priorità 10.000
  - Regola A2: priorità 20.000

- Regola 2 — priorità 200
- RuleGroupB — priorità 300
  - Regola B1 — priorità 0
  - Regola B2 — priorità 1

AWS WAF valuterebbe le regole per questo ACL web nel seguente ordine:

- Regola 1
- RuleGroupUna regola A1
- RuleGroupUna regola A2
- Regola 2
- RuleGroupRegola B B1
- RuleGroupRegola B B2

Come vengono gestite le azioni delle regole e dei gruppi di regole in un ACL Web

Quando configuri le regole e i gruppi di regole, scegli come AWS WAF gestire le richieste web corrispondenti:

- Allowe Block stanno terminando le azioni Allow e le Block azioni interrompono tutte le altre elaborazioni dell'ACL web sulla richiesta web corrispondente. Se una regola in un ACL Web trova una corrispondenza per una richiesta e l'azione della regola è Allow oBlock, tale corrispondenza determina la disposizione finale della richiesta Web per l'ACL Web. AWS WAF non elabora altre regole nell'ACL web successive a quella corrispondente. Ciò vale per le regole che aggiungi direttamente all'ACL Web e le regole che si trovano all'interno di un gruppo di regole aggiunto. Con l'Blockazione, la risorsa protetta non riceve o elabora la richiesta web.
- Countè un'azione non terminante: quando una regola con un'Countazione corrisponde a una richiesta, AWS WAF conta la richiesta, quindi continua a elaborare le regole che seguono nel set di regole ACL Web.
- CAPTCHAe Challenge può essere un'azione che non termina o termina: quando una regola con una di queste azioni corrisponde a una richiesta, ne verifica lo stato del token. AWS WAF Se la richiesta ha un token valido, AWS WAF considera la corrispondenza come una Count corrispondenza e quindi continua a elaborare le regole che seguono nel set di regole ACL Web. Se la richiesta non ha un token valido, AWS WAF interrompe la valutazione e invia al client un puzzle CAPTCHA o una sfida di sessione client in background silenziosa da risolvere.

Se la valutazione della regola non comporta alcuna azione di interruzione, AWS WAF applica l'azione Web ACL predefinita alla richiesta. Per informazioni, consulta L'azione predefinita dell'ACL Web.

Nel tuo ACL web, puoi sovrascrivere le impostazioni di azione per le regole all'interno di un gruppo di regole e puoi sovrascrivere l'azione restituita da un gruppo di regole. Per informazioni, consulta Le azioni sostituiscono i gruppi di regole.

Interazione tra azioni e impostazioni di priorità

Le azioni che AWS WAF si applicano a una richiesta Web sono influenzate dalle impostazioni di priorità numerica delle regole nell'ACL Web. Ad esempio, supponiamo che l'ACL Web abbia una regola con Allow azione e priorità numerica di 50 e un'altra regola con Count azione e priorità numerica di 100. AWS WAF valuta le regole in un ACL Web in base all'ordine di priorità, a partire dall'impostazione più bassa, in modo da valutare la regola di autorizzazione prima della regola di conteggio. Una richiesta web che corrisponde a entrambe le regole corrisponderà per prima alla regola di autorizzazione. Trattandosi di Allow un'azione terminante, AWS WAF interromperà la valutazione in questa partita e non valuterà la richiesta in base alla regola di conteggio.

- Se desideri includere solo le richieste che non corrispondono alla regola di autorizzazione nelle metriche delle regole di conteggio, le impostazioni di priorità delle regole funzionerebbero.
- D'altra parte, se desideri che le metriche di conteggio contenute nella regola di conteggio vengano applicate anche alle richieste che corrispondono alla regola di autorizzazione, devi assegnare alla regola di conteggio un'impostazione di priorità numerica inferiore rispetto alla regola di autorizzazione, in modo che venga eseguita per prime.

Per ulteriori informazioni sulle impostazioni di priorità, consulta. Ordine di elaborazione delle regole e dei gruppi di regole in un ACL Web

Le azioni sostituiscono i gruppi di regole

Quando aggiungi un gruppo di regole all'ACL Web, puoi ignorare le azioni eseguite sulle richieste Web corrispondenti. La sovrascrittura delle azioni per un gruppo di regole all'interno della configurazione ACL Web non altera il gruppo di regole stesso. Modifica solo il modo in cui AWS WAF utilizza il gruppo di regole nel contesto dell'ACL web.

L'azione delle regole ha la precedenza

È possibile sostituire le azioni delle regole all'interno di un gruppo di regole sostituendo qualsiasi azione valida. Quando si esegue questa operazione, le richieste corrispondenti vengono gestite esattamente come se l'azione della regola configurata fosse l'impostazione di override.

> **Note**
>
> Le azioni delle regole possono essere terminative o non terminative. Un'azione di terminazione interrompe la valutazione ACL Web della richiesta e consente alla richiesta di continuare verso l'applicazione protetta oppure la blocca.

Di seguito sono riportate le opzioni dell'operazione delle regole:

- Allow— AWS WAF consente di inoltrare la richiesta alla AWS risorsa protetta per l'elaborazione e la risposta. Si tratta di un'azione terminativa. Nelle regole che definisci, puoi inserire intestazioni personalizzate nella richiesta prima di inoltrarla alla risorsa protetta.
- Block— AWS WAF blocca la richiesta. Si tratta di un'azione terminativa. Per impostazione predefinita, la AWS risorsa protetta risponde con un codice di `403 (Forbidden)` stato HTTP. Nelle regole che definisci, puoi personalizzare la risposta. Quando AWS WAF blocca una richiesta, le impostazioni dell'Blockazione determinano la risposta che la risorsa protetta invia al client.
- Count— AWS WAF conta la richiesta ma non determina se consentirla o bloccarla. Si tratta di un'azione non terminante. AWS WAF continua a elaborare le regole rimanenti nell'ACL Web. Nelle regole che definisci, puoi inserire intestazioni personalizzate nella richiesta e aggiungere etichette alle quali altre regole possono corrispondere.
- CAPTCHAe Challenge — AWS WAF utilizza i puzzle CAPTCHA e le sfide silenziose per verificare che la richiesta non provenga da un bot e AWS WAF utilizza i token per tenere traccia delle recenti risposte positive dei clienti.

> **Note**
>
> Ti vengono addebitati costi aggiuntivi quando utilizzi l'azione CAPTCHA o Challenge regola in una delle tue regole o come regola che sostituisce un'azione in un gruppo di regole. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

Queste azioni sulle regole possono terminare o non terminare, a seconda dello stato del token nella richiesta:

- Non terminazione per un token valido e non scaduto: se il token è valido e non è scaduto in base al CAPTCHA configurato o al tempo di immunità alla sfida, gestisce la richiesta in modo simile all'azione. AWS WAF Count AWS WAF continua a controllare la richiesta web in base alle regole rimanenti nell'ACL web. Analogamente alla Count configurazione, nelle regole da voi definite potete facoltativamente configurare queste azioni con intestazioni personalizzate da inserire nella richiesta e aggiungere etichette alle quali altre regole possono corrispondere.
- Terminazione con una richiesta bloccata per un token non valido o scaduto: se il token non è valido o il timestamp indicato è scaduto, AWS WAF interrompe l'ispezione della richiesta Web e blocca la richiesta, analogamente all'azione. Block AWS WAF quindi risponde al client con un codice di risposta personalizzato. InfattiCAPTCHA, se il contenuto della richiesta indica che il browser del client è in grado di gestirla, AWS WAF invia un puzzle CAPTCHA in formato JavaScript interstiziale, progettato per distinguere i client umani dai bot. Per l'Challengeazione, AWS WAF invia un messaggio JavaScript interstitial con una sfida silenziosa progettata per distinguere i browser normali dalle sessioni gestite dai bot.

Per ulteriori informazioni, consulta CAPTCHAe Challenge in AWS WAF.

Per informazioni su come utilizzare questa opzione, consulta. Sovrascrivere le azioni delle regole in un gruppo di regole

Sovrascrivere l'azione della regola in Count

Il caso d'uso più comune per sostituire le azioni delle regole consiste nel sovrascrivere alcune o tutte le azioni delle regole per Count testare e monitorare il comportamento di un gruppo di regole prima di metterlo in produzione.

Puoi anche usarlo per risolvere i problemi di un gruppo di regole che genera falsi positivi. I falsi positivi si verificano quando un gruppo di regole blocca il traffico che non ti aspetti che blocchi. Se identifichi una regola all'interno di un gruppo di regole che bloccherebbe le richieste che desideri consentire l'accesso, puoi mantenere l'azione count override su quella regola, per escluderla dall'agire sulle tue richieste.

Per ulteriori informazioni sull'utilizzo della regola Action Override nei test, consulta. Test e ottimizzazione delle protezioni AWS WAF

Elenco JSON: sostituisce **`RuleActionOverridesExcludedRules`**

Se hai impostato le azioni relative alle regole del gruppo di regole Count nella configurazione dell'ACL Web prima del 27 ottobre 2022, AWS WAF hai salvato le sostituzioni nell'ACL Web JSON come. `ExcludedRules` Ora, l'impostazione JSON per sovrascrivere una regola si trova nelle impostazioni. Count `RuleActionOverrides`

Quando si utilizza la AWS WAF console per modificare le impostazioni esistenti del gruppo di regole, la console converte automaticamente tutte `ExcludedRules` le impostazioni del JSON in `RuleActionOverrides` impostazioni, con l'azione di override impostata su. Count

- Esempio di impostazione corrente:

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

- Vecchio esempio di impostazione:

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

Ti consigliamo di aggiornare tutte le `ExcludedRules` impostazioni nelle tue inserzioni JSON alle `RuleActionOverrides` impostazioni con l'azione impostata su. Count L'API accetta entrambe le

impostazioni, ma se utilizzi solo la nuova `RuleActionOverrides` impostazione, otterrai la coerenza nelle tue inserzioni JSON tra il funzionamento della console e il funzionamento dell'API.

L'azione di gruppo di regole viene sostituita da Count

È possibile sovrascrivere l'azione restituita dal gruppo di regole, impostandola su. Count

> **Note**
>
> Questa non è una buona opzione per testare le regole in un gruppo di regole, perché non altera il modo in cui AWS WAF valuta il gruppo di regole stesso. Influisce solo sul modo in cui AWS WAF gestisce i risultati restituiti all'ACL Web dalla valutazione del gruppo di regole. Se vuoi testare le regole in un gruppo di regole, usa l'opzione descritta nella sezione precedente,. L'azione delle regole ha la precedenza

Quando si sostituisce l'azione del gruppo di regole suCount, AWS WAF elabora normalmente la valutazione del gruppo di regole.

Se nessuna regola nel gruppo di regole corrisponde o se tutte le regole di corrispondenza hanno un'Countazione, questa sostituzione non ha alcun effetto sull'elaborazione del gruppo di regole o dell'ACL web.

La prima regola del gruppo di regole che corrisponde a una richiesta Web e che presenta un'azione di terminazione causa l'interruzione della valutazione del gruppo AWS WAF di regole e restituisce il risultato dell'azione di terminazione al livello di valutazione dell'ACL Web. A questo punto, nella valutazione dell'ACL web, questo override ha effetto. AWS WAF sostituisce l'azione di terminazione in modo che il risultato della valutazione del gruppo di regole sia solo un'azione. Count AWS WAF quindi continua a elaborare il resto delle regole nell'ACL Web.

Per informazioni su come utilizzare questa opzione, vedereSovrascrivere il risultato della valutazione di un gruppo di regole con Count.

L'azione predefinita dell'ACL Web

Quando si crea e si configura un ACL Web, è necessario impostare l'azione predefinita dell'ACL Web. AWS WAF applica questa azione a qualsiasi richiesta Web che superi tutte le valutazioni delle regole dell'ACL Web senza che venga applicata un'azione di terminazione. Un'azione di terminazione interrompe la valutazione dell'ACL Web della richiesta e la consente di continuare sull'applicazione protetta o la blocca. Per informazioni sulle azioni delle regole, vedere. Operazione delle regole

L'azione Web ACL predefinita deve determinare la disposizione finale della richiesta Web, quindi è un'azione terminativa:

- Allow— Se desideri consentire alla maggior parte degli utenti di accedere al tuo sito Web, ma desideri bloccare l'accesso agli aggressori le cui richieste provengono da indirizzi IP specifici o le cui richieste sembrano contenere codice SQL dannoso o valori specifici, scegli Allow l'azione predefinita. Quindi, quando aggiungi regole all'ACL Web, assicurati che identifichino e blocchino le richieste specifiche che desideri bloccare. Con questa azione, puoi inserire intestazioni personalizzate nella richiesta prima di inoltrarla alla risorsa protetta.
- Block— Se desideri impedire alla maggior parte degli utenti di accedere al tuo sito Web, ma desideri consentire l'accesso agli utenti le cui richieste provengono da indirizzi IP specifici o le cui richieste contengono valori specifici, scegli Block l'azione predefinita. Quindi, quando aggiungi regole all'ACL Web, assicurati che identifichino e consentano le richieste specifiche che desideri consentire. Per impostazione predefinita, per l'Blockazione, la AWS risorsa risponde con un codice di `403 (Forbidden)` stato HTTP, ma è possibile personalizzare la risposta.

Per informazioni sulla personalizzazione delle richieste e delle risposte, consulta. Richieste e risposte web personalizzate in AWS WAF

La configurazione delle regole e dei gruppi di regole varia a seconda che si desideri consentire o bloccare la maggior parte delle richieste Web. Ad esempio, se desideri consentire la maggior parte delle richieste, devi impostare l'azione predefinita Web ACL su e quindi aggiungere regole che identificano le richieste Web da bloccare, come le seguenti: Allow

- Richieste che hanno origine da indirizzi IP che stanno effettuando un numero irragionevole di richieste
- Richieste che hanno origine da paesi nei quali non operi o che sono frequenti fonti di attacchi
- Richieste che includono valori falsi nell'intestazione `User-agent`
- Richieste che sembrano includere codice SQL dannoso

Le regole gestite dei gruppi di regole in genere utilizzano l'Blockazione, ma non tutte la utilizzano. Ad esempio, alcune regole utilizzate per Bot Control utilizzano le impostazioni CAPTCHA e Challenge action. Per informazioni sui gruppi di regole gestite, consulta Gruppi di regole gestite.

Gestione dei limiti di dimensione delle ispezioni corporee

Il limite di dimensione del corpo sottoposto a ispezione è la dimensione massima del corpo richiesto che AWS WAF è possibile ispezionare. Quando il corpo di una richiesta Web supera il limite, il servizio host sottostante inoltra solo i contenuti che rientrano nel limite consentito AWS WAF per l'ispezione.

- Per Application Load Balancer and AWS AppSync, il limite è fissato a 8 KB (8.192 byte).
- Per CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, il limite predefinito è 16 KB (16.384 byte) e puoi aumentare il limite per qualsiasi tipo di risorsa con incrementi di 16 KB, fino a 64 KB. Le opzioni di impostazione sono 16 KB, 32 KB, 48 KB e 64 KB.

Manipolazione di corpi di grandi dimensioni

Se il traffico web include corpi che superano il limite, verrà applicata la gestione delle sovradimensionate configurata. Per informazioni sulle opzioni per la gestione delle dimensioni eccessive, consulta. Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF

Considerazioni sui prezzi per gli aumenti dei limiti

AWS WAF addebita una tariffa base per l'ispezione del traffico che rientra nel limite predefinito per il tipo di risorsa.

Per le CloudFront risorse API Gateway, Amazon Cognito, App Runner e Verified Access, se aumenti l'impostazione del limite, il traffico che AWS WAF puoi ispezionare include le dimensioni del corpo fino al nuovo limite. Ti viene addebitato un costo aggiuntivo solo per l'ispezione delle richieste con dimensioni corporee superiori ai 16 KB predefiniti. Per ulteriori informazioni sui prezzi, consulta Prezzi di AWS WAF.

Come modificare il limite di dimensione per l'ispezione dell'organismo

Puoi configurare il limite di dimensione dell'ispezione corporea per CloudFront le risorse API Gateway, Amazon Cognito, App Runner o Verified Access.

Quando crei o modifichi un ACL web, puoi modificare i limiti delle dimensioni di body inspection nella configurazione dell'associazione delle risorse. Per l'API, consulta la configurazione dell'associazione dell'ACL Web all'indirizzo. AssociationConfig Per la console, consultate la configurazione nella pagina in cui specificate le risorse associate all'ACL Web. Per indicazioni sulla configurazione della console, consultaUtilizzo delle ACL Web.

Configurazione del dominio CAPTCHA, challenge e token per un ACL web

È possibile configurare le opzioni nell'ACL Web per le regole che utilizzano le azioni delle Challenge regole CAPTCHA o e per gli SDK di integrazione delle applicazioni che gestiscono le sfide silenziose dei client per le protezioni gestite. AWS WAF

Queste funzionalità mitigano l'attività dei bot sfidando gli utenti finali con puzzle CAPTCHA e presentando alle sessioni client sfide silenziose. Quando il client risponde con successo, AWS WAF fornisce un token da utilizzare nella richiesta web, con data e ora dell'ultima risposta riuscita al puzzle e alla sfida. Per ulteriori informazioni, consulta AWS WAF mitigazione intelligente delle minacce.

Nella configurazione Web ACL, puoi configurare come gestire questi token: AWS WAF

- Tempi di immunità al CAPTCHA e alle sfide: specificano per quanto tempo un CAPTCHA o un timestamp della sfida rimane valido. Le impostazioni Web ACL vengono ereditate da tutte le regole che non dispongono di impostazioni relative al tempo di immunità configurate e anche dagli SDK di integrazione delle applicazioni. Per ulteriori informazioni, consulta Scadenza del timestamp: tempi di immunità dei token.
- Domini token: per impostazione predefinita, AWS WAF accetta i token solo per il dominio della risorsa a cui è associato l'ACL Web. Se configuri un elenco di domini token, AWS WAF accetta token per tutti i domini dell'elenco e per il dominio della risorsa associata. Per ulteriori informazioni, consulta Configurazione dell'elenco dei domini del token ACL Web.

Utilizzo delle ACL Web

Questa sezione fornisce le procedure per la creazione, la gestione e l'utilizzo degli ACL Web tramite la AWS console.

Per qualsiasi ACL Web che stai utilizzando, puoi accedere ai riepiloghi delle metriche del traffico Web nella pagina dell'ACL Web nella AWS WAF console, nella scheda Panoramica del traffico. Le dashboard della console forniscono riepiloghi quasi in tempo reale delle CloudWatch metriche di Amazon AWS WAF raccolte durante la valutazione del traffico web dell'applicazione. Per ulteriori informazioni sui dashboard, consulta. Dashboard di panoramica sul traffico ACL Web Per ulteriori informazioni sul monitoraggio del traffico dell'ACL Web, consulta. Monitoraggio e ottimizzazione

Rischio legato al traffico di produzione

Prima di implementare modifiche all'ACL Web per il traffico di produzione, testale e ottimizzale in un ambiente di staging o di test finché non ti rendi conto del potenziale impatto sul traffico. Quindi testa e ottimizza le regole aggiornate in modalità di conteggio con il traffico di produzione prima di attivarle. Per le linee guida, consulta Test e ottimizzazione delle protezioni AWS WAF.

Note

L'utilizzo di più di 1.500 WCU in un ACL Web comporta costi superiori al prezzo base dell'ACL Web. Per ulteriori informazioni, consulta AWS WAF unità di capacità Web ACL (WCU) e Prezzi di AWS WAF.

Incoerenze temporanee durante gli aggiornamenti

Quando si crea o si modifica un ACL Web o altre AWS WAF risorse, le modifiche richiedono poco tempo per essere propagate in tutte le aree in cui sono archiviate le risorse. Il tempo di propagazione può variare da pochi secondi a diversi minuti.

Di seguito sono riportati alcuni esempi delle incongruenze temporanee che potreste notare durante la propagazione delle modifiche:

- Dopo aver creato un ACL Web, se si tenta di associarlo a una risorsa, è possibile che venga visualizzata un'eccezione che indica che l'ACL Web non è disponibile.
- Dopo aver aggiunto un gruppo di regole a un ACL Web, le nuove regole del gruppo di regole potrebbero essere in vigore in un'area in cui viene utilizzato l'ACL Web e non in un'altra.
- Dopo aver modificato l'impostazione di un'azione della regola, è possibile vedere la vecchia azione in alcuni punti e la nuova azione in altri.
- Dopo aver aggiunto un indirizzo IP a un set IP utilizzato in una regola di blocco, il nuovo indirizzo potrebbe essere bloccato in un'area mentre è ancora consentito in un'altra.

Argomenti

- Gestione del comportamento del gruppo di regole in un'ACL Web
- Associazione o dissociazione di un ACL Web con una risorsa AWS
- Eliminazione di un ACL Web

Creazione di un'ACL Web

Per creare un nuovo ACL Web, utilizzare la procedura guidata per la creazione di ACL Web seguendo la procedura riportata in questa pagina.

> **Rischio legato al traffico di produzione**
>
> Prima di implementare modifiche all'ACL Web per il traffico di produzione, testale e ottimizzale in un ambiente di staging o di test finché non ti rendi conto del potenziale impatto sul traffico. Quindi testa e ottimizza le regole aggiornate in modalità di conteggio con il traffico di produzione prima di attivarle. Per le linee guida, consulta Test e ottimizzazione delle protezioni AWS WAF.

> **Note**
>
> L'utilizzo di più di 1.500 WCU in un ACL Web comporta costi superiori al prezzo base dell'ACL Web. Per ulteriori informazioni, consulta AWS WAF unità di capacità Web ACL (WCU) e Prezzi di AWS WAF.

Per creare un'ACL Web

1. Accedi AWS Management Console e apri la console all'indirizzo https://console.aws.amazon.com/wafv2/. AWS WAF
2. Scegliere Web ACLs (ACL Web) nel riquadro di navigazione e selezionare Create web ACL (Crea ACL Web).
3. Per Name (Nome), immettere il nome che si desidera utilizzare per identificare l'ACL Web.

   > **Note**
   >
   > Non è possibile modificare il nome dopo aver creato l'ACL Web.

4. (Facoltativo) Per Description - optional (Descrizione - facoltativo), immettere una descrizione più lunga per l'ACL Web, se richiesta.
5. Per il nome della CloudWatch metrica, modifica il nome predefinito, se applicabile. Seguire le linee guida sulla console per i caratteri validi. Il nome non può contenere caratteri speciali, spazi bianchi o nomi di metriche riservati AWS WAF, inclusi «All» e «Default_Action».

   > **Note**
   >
   > Non è possibile modificare il nome della CloudWatch metrica dopo aver creato l'ACL Web.

6. In Tipo di risorsa, scegli la categoria di AWS risorsa che desideri associare a questo ACL web, CloudFront distribuzioni Amazon o risorse regionali. Per ulteriori informazioni, consulta Associazione o dissociazione di un ACL Web con una risorsa AWS.
7. Per Regione, se hai scelto un tipo di risorsa regionale, scegli la regione in cui desideri AWS WAF archiviare l'ACL web.

   Devi scegliere questa opzione solo per i tipi di risorse regionali. Per CloudFront le distribuzioni, la regione è codificata nella regione Stati Uniti orientali (Virginia settentrionale)`us-east-1`, per le applicazioni Global (). CloudFront
8. (CloudFront, API Gateway, Amazon Cognito, App Runner e Verified Access) Per il limite di dimensione dell'ispezione delle richieste Web: facoltativo, se desideri specificare un limite di dimensione diverso per l'ispezione corporea, seleziona il limite. L'ispezione di dimensioni del corpo superiori al valore predefinito di 16 KB può comportare costi aggiuntivi. Per ulteriori informazioni su questa opzione, consulta Gestione dei limiti di dimensione delle ispezioni corporee.
9. (Facoltativo) Per AWS Risorse associate: facoltativo, se desideri specificare subito le tue risorse, scegli Aggiungi risorse. AWS Nella finestra di dialogo, scegli le risorse che desideri associare, quindi scegli Aggiungi. AWS WAF torna alla pagina Descrivi web ACL e AWS risorse associate.
10. Seleziona Successivo.
11. (Facoltativo) Se si desidera aggiungere gruppi di regole gestite, nella pagina Add rules and rule groups (Aggiungi regole e gruppi di regole), scegliere Add rules (Aggiungi regole), quindi Add managed rule groups (Aggiungi gruppi di regole gestite). Eseguire le seguenti operazioni per ogni gruppo di regole gestite che si desidera aggiungere:

a. Nella pagina Aggiungi gruppi di regole gestiti, espandi l'elenco per i gruppi di regole AWS gestiti o per il Marketplace AWS venditore di tua scelta.

b. Per il gruppo di regole che desideri aggiungere, nella colonna Azione, attiva l'opzione Aggiungi al web ACL.

   Per personalizzare il modo in cui l'ACL Web utilizza il gruppo di regole, scegli Modifica. Di seguito sono riportate le impostazioni di personalizzazione più comuni:

   - Sostituisci le azioni delle regole per alcune o tutte le regole. Se non si definisce un'azione di sostituzione per una regola, la valutazione utilizza l'azione della regola definita all'interno del gruppo di regole. Per ulteriori informazioni su questa opzione, consulta Le azioni sostituiscono i gruppi di regole.
   - Riduci l'ambito delle richieste Web esaminate dal gruppo di regole aggiungendo un'istruzione scope-down. Per ulteriori informazioni su questa opzione, consulta Dichiarazioni delimitate.
   - Alcuni gruppi di regole gestiti richiedono una configurazione aggiuntiva. Consulta la documentazione del tuo fornitore di gruppi di regole gestiti. Per informazioni specifiche sui gruppi di regole AWS Managed Rules, consultaAWS Regole gestite per AWS WAF.

   Quando hai finito con le impostazioni, scegli Salva regola.

Scegliere Add rules (Aggiungi regole) per completare l'aggiunta di regole gestite e tornare alla pagina Add rules and rule groups (Aggiungi regole e gruppi di regole).

12. (Facoltativo) Se si desidera aggiungere un proprio gruppo di regole, nella pagina Add rules and rule groups (Aggiungi regole e gruppi di regole), scegliere Add rules (Aggiungi regole), quindi selezionare Add my own rules and rule groups (Aggiungi le mie regole e i miei gruppi di regole). Eseguire le seguenti operazioni per ogni gruppo di regole che si desidera aggiungere:

    a. Nella pagina Add my own rules and rule groups (Aggiungi le mie regole e i miei gruppi di regole), scegliere Rule group (Gruppo di regole).

    b. Per Nome, inserisci il nome che desideri utilizzare per la regola del gruppo di regole in questo ACL web. Non utilizzare nomi che iniziano con`AWS`, `ShieldPreFM`, o`PostFM`. Queste stringhe sono riservate o potrebbero creare confusione con i gruppi di regole gestiti dall'utente da altri servizi. Per informazioni, consulta Gruppi di regole forniti da altri servizi.

    c. Scegliere il gruppo di regole dall'elenco.

> **Note**
>
> Se desideri sovrascrivere le azioni delle regole per un tuo gruppo di regole, salvalo prima nell'ACL Web, quindi modifica l'ACL Web e la dichiarazione di riferimento del gruppo di regole nell'elenco delle regole dell'ACL Web. È possibile sostituire le azioni delle regole con qualsiasi impostazione di azione valida, come si può fare per i gruppi di regole gestiti.

d. Scegli Aggiungi regola.

13. (Facoltativo) Se si desidera aggiungere la propria regola, nella pagina Add rules and rule groups (Aggiungi regole e gruppi di regole), scegliere Add rules (Aggiungi regole), Add my own rules and rule groups (Aggiungi le mie regole e i miei gruppi di regole), Rule builder (Generatore di regole), quindi Rule visual editor (Editor visivo delle regole).

> **Note**
>
> Il Rule visual editor (Editor visivo delle regole) della console supporta un livello di nidificazione. Ad esempio, è possibile utilizzare una singola `OR` istruzione `AND` o logica e inserire al suo interno un livello di altre istruzioni, ma non è possibile annidare istruzioni logiche all'interno di istruzioni logiche. Per gestire istruzioni delle regole più complesse, utilizzare Rule JSON editor (Editor JSON delle regole). Per informazioni su tutte le opzioni per le regole, consulta AWS WAF regole.
> Questa procedura descrive il Rule visual editor (Editor visivo delle regole).

a. In Name (Nome), immettere il nome che si desidera utilizzare per identificare questa regola. Non utilizzare nomi che iniziano con `AWSShield`,`PreFM`, o`PostFM`. Queste stringhe sono riservate o potrebbero creare confusione con i gruppi di regole gestiti dall'utente da altri servizi.

b. Immettere la definizione della regola, in base alle proprie esigenze. È possibile combinare regole all'interno di istruzioni logiche `AND` e di `OR` regole. La procedura guidata descrive le opzioni per ogni regola, a seconda del contesto. Per informazioni sulle opzioni delle regole, consulta AWS WAF regole.

c. In Action (Operazione), selezionare l'operazione che deve essere eseguita dalla regola quando corrisponde a una richiesta Web. Per informazioni sulle scelte, consulta Operazione delle regole e Valutazione delle regole ACL Web e dei gruppi di regole.

Se si utilizza l'Challengeazione CAPTCHAo, modificare la configurazione del tempo di immunità in base alle esigenze della regola. Se non specifichi l'impostazione, la regola la eredita dall'ACL web. Per modificare le impostazioni relative al tempo di immunità ACL Web, modifica l'ACL Web dopo averlo creato. Per ulteriori informazioni sui tempi di immunità, vedere. Scadenza del timestamp: tempi di immunità dei token

> **Note**
>
> Ti vengono addebitati costi aggiuntivi quando utilizzi l'azione CAPTCHA o Challenge in una delle tue regole o come regola che sostituisce un'azione in un gruppo di regole. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

Se desideri personalizzare la richiesta o la risposta, scegli le relative opzioni e inserisci i dettagli della personalizzazione. Per ulteriori informazioni, consulta Richieste e risposte web personalizzate in AWS WAF.

Se desideri che la tua regola aggiunga etichette alle richieste web corrispondenti, scegli le relative opzioni e inserisci i dettagli dell'etichetta. Per ulteriori informazioni, consulta AWS WAF etichette sulle richieste web.

d. Scegli Aggiungi regola.

14. Scegli l'azione predefinita per l'ACL web, Block oppureAllow. Questa è l'azione che viene AWS WAF eseguita su una richiesta quando le regole dell'ACL Web non la consentono o la bloccano esplicitamente. Per ulteriori informazioni, consulta L'azione predefinita dell'ACL Web.

    Se desideri personalizzare l'azione predefinita, scegli le relative opzioni e inserisci i dettagli della personalizzazione. Per ulteriori informazioni, consulta Richieste e risposte web personalizzate in AWS WAF.

15. È possibile definire un elenco di domini Token per abilitare la condivisione dei token tra applicazioni protette. I token vengono utilizzati dalle Challenge azioni CAPTCHA e e dagli SDK di integrazione delle applicazioni implementati quando si utilizzano i gruppi di regole AWS Managed Rules per AWS WAF Fraud Control, la prevenzione delle frodi (ACFP), la prevenzione delle frodi di account AWS WAF Fraud Control (ATP) e il controllo dei bot. AWS WAF

    I suffissi pubblici non sono consentiti. Ad esempio, non puoi usare `gov.au` or `co.uk` come dominio token.

Per impostazione predefinita, AWS WAF accetta token solo per il dominio della risorsa protetta. Se aggiungi domini token in questo elenco, AWS WAF accetta token per tutti i domini dell'elenco e per il dominio della risorsa associata. Per ulteriori informazioni, consulta la pagina Configurazione dell'elenco dei domini del token ACL Web.

16. Seleziona Next (Successivo).
17. Nella pagina Imposta la priorità delle regole, seleziona e sposta le regole e i gruppi di regole nell'ordine in cui desideri AWS WAF elaborarli. AWS WAF elabora le regole a partire dall'inizio dell'elenco. Quando si salva il Web, ACL AWS WAF assegna le impostazioni di priorità numerica alle regole, nell'ordine in cui sono elencate. Per ulteriori informazioni, consulta la pagina Ordine di elaborazione delle regole e dei gruppi di regole in un ACL Web.
18. Seleziona Next (Successivo).
19. Nella pagina Configura le metriche, esamina le opzioni e applica gli aggiornamenti necessari. Puoi combinare metriche provenienti da più fonti fornendo loro lo stesso nome di CloudWatch metrica.
20. Seleziona Successivo.
21. Nella pagina Review and create Web ACL (Rivedi e crea ACL Web), controllare le definizioni. Se si desidera modificare un'area qualsiasi, scegliere Edit (Modifica) per l'area. Viene visualizzata di nuovo la pagina nella procedura guidata ACL Web. Apportare le eventuali modifiche, quindi scegliere Next (Avanti) nelle varie pagine fino a tornare alla pagina Review and create web ACL (Rivedi e crea ACL Web) .
22. Scegliere Create web ACL (Crea ACL Web). La nuova ACL Web è elencata nella pagina Web ACLs (ACL Web) .

Modifica di un ACL Web

Per aggiungere o rimuovere regole da un ACL Web o modificare le impostazioni di configurazione, accedi all'ACL Web utilizzando la procedura riportata in questa pagina. Durante l'aggiornamento di un ACL Web, AWS WAF fornisce una copertura continua alle risorse associate all'ACL Web.

⚠ Rischio legato al traffico di produzione

Prima di implementare modifiche all'ACL Web per il traffico di produzione, testale e ottimizzale in un ambiente di staging o di test finché non ti senti a tuo agio con il potenziale impatto sul traffico. Quindi testa e ottimizza le regole aggiornate in modalità di conteggio con

il traffico di produzione prima di abilitarle. Per le linee guida, consulta Test e ottimizzazione delle protezioni AWS WAF.

> **Note**
>
> L'utilizzo di più di 1.500 WCU in un ACL Web comporta costi superiori al prezzo base dell'ACL Web. Per ulteriori informazioni, consulta AWS WAF unità di capacità Web ACL (WCU) e Prezzi di AWS WAF.

Per modificare un'ACL Web

1. Accedi AWS Management Console e apri la console all'indirizzo https://console.aws.amazon.com/wafv2/. AWS WAF
2. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).
3. Scegliere l'ACL Web che si desidera modificare. La console ti porta alla descrizione dell'ACL Web.

   > **Note**
   >
   > Gli ACL Web gestiti da AWS Firewall Manager hanno nomi che iniziano con. `FMManagedWebACLV2-` L'amministratore di Firewall Manager li gestisce nelle AWS WAF politiche di Firewall Manager. Queste ACL Web potrebbero contenere set di gruppi di regole che sono designati per essere eseguiti per primi e per ultimi nell'ACL Web, su entrambi i lati di regole o gruppi di regole aggiunti e gestiti. Non è possibile modificare nessuna di queste specifiche del primo e dell'ultimo gruppo di regole. Il primo e l'ultimo gruppo di regole hanno nomi che iniziano `POSTFMManaged-` rispettivamente con `PREFMManaged-` e. Per ulteriori informazioni su questo tipo di policy, consulta AWS WAF politiche.
4. Modificate l'ACL Web in base alle esigenze. Seleziona le schede per le aree di configurazione che ti interessano e modifica le impostazioni modificabili. Per ogni impostazione che modifichi, quando scegli Salva e torni alla pagina di descrizione dell'ACL Web, la console salva le modifiche all'ACL Web.

   Di seguito sono elencate le schede che contengono i componenti di configurazione Web ACL.

- Scheda Regole
  - Regole definite nell'ACL Web: puoi modificare e gestire le regole che hai definito nell'ACL Web in modo simile a come hai fatto durante la creazione dell'ACL Web.

    > **Note**
    >
    > Non modificate i nomi delle regole che non avete aggiunto manualmente all'ACL web. Se utilizzi altri servizi per gestire le regole al tuo posto, la modifica dei loro nomi potrebbe rimuovere o ridurre la loro capacità di fornire le protezioni previste. AWS Shield Advanced ed AWS Firewall Manager entrambi creano regole nell'ACL web. Per informazioni, consulta Gruppi di regole forniti da altri servizi.

    > **Note**
    >
    > Se modifichi il nome di una regola e desideri che il nome della metrica della regola rifletta la modifica, devi aggiornare anche il nome della metrica. AWS WAF non aggiorna automaticamente il nome della metrica di una regola quando si modifica il nome della regola. Puoi cambiare il nome della metrica quando modifichi la regola nella console, utilizzando l'editor JSON delle regole. Puoi anche modificare entrambi i nomi tramite le API e in qualsiasi elenco JSON che utilizzi per definire l'ACL web o il gruppo di regole.

    Per informazioni sulle regole e sulle impostazioni dei gruppi di regole, consulta e. AWS WAF regole Gruppi di regole
  - Unità di capacità della regola Web ACL utilizzate: l'attuale utilizzo della capacità per l'ACL Web. Questa è di sola visualizzazione.
  - Azione ACL Web predefinita per le richieste che non corrispondono a nessuna regola: per informazioni su questa impostazione, consultaL'azione predefinita dell'ACL Web.
  - Configurazioni Web ACL CAPTCHA e challenge: questi tempi di immunità determinano per quanto tempo un CAPTCHA o un token di sfida rimane valido dopo l'acquisizione. Puoi modificare questa impostazione solo qui, dopo aver creato l'ACL web. Per informazioni su queste impostazioni, consulta Scadenza del timestamp: tempi di immunità dei token.

    - Elenco di domini token: AWS WAF accetta token per tutti i domini dell'elenco e per il dominio della risorsa associata. Per ulteriori informazioni, consulta Configurazione dell'elenco dei domini del token ACL Web.
- Scheda Risorse associate AWS
    - Limite di dimensione per l'ispezione delle richieste Web: incluso solo per gli ACL Web che proteggono le CloudFront distribuzioni. Il limite di dimensione per l'ispezione della carrozzeria determina la quantità di componente del corpo destinata all'ispezione. AWS WAF Per ulteriori informazioni su questa impostazione, consulta Gestione dei limiti di dimensione delle ispezioni corporee.
    - AWS Risorse associate: l'elenco delle risorse a cui l'ACL Web è attualmente associato e protetto. È possibile individuare le risorse che si trovano all'interno della stessa regione dell'ACL Web e associarle all'ACL Web. Per ulteriori informazioni, consulta Associazione o dissociazione di un ACL Web con una risorsa AWS.
- Scheda Corpi di risposta personalizzati
    - Corpi di risposta personalizzati che possono essere utilizzati dalle regole ACL Web con l'azione impostata su. Block Per ulteriori informazioni, consulta Risposte personalizzate per Block le azioni.
- Scheda Registrazione e metriche
    - Registrazione: registrazione del traffico valutato dall'ACL Web. Per informazioni, consulta Registrazione del traffico AWS WAF ACL Web.
    - Richieste campionate: informazioni sulle regole che corrispondono alle richieste Web. Per informazioni sulla visualizzazione delle richieste campionate, vedere. Visualizzazione di un esempio di richieste Web
    - CloudWatch metriche: metriche per le regole nell'ACL Web. Per informazioni sui CloudWatch parametri di Amazon, consultaMonitoraggio con Amazon CloudWatch.

Incoerenze temporanee durante gli aggiornamenti

Quando si crea o si modifica un ACL Web o altre AWS WAF risorse, le modifiche richiedono poco tempo per essere propagate in tutte le aree in cui sono archiviate le risorse. Il tempo di propagazione può variare da pochi secondi a diversi minuti.

Di seguito sono riportati alcuni esempi delle incongruenze temporanee che potreste notare durante la propagazione delle modifiche:

- Dopo aver creato un ACL Web, se si tenta di associarlo a una risorsa, è possibile che venga visualizzata un'eccezione che indica che l'ACL Web non è disponibile.
- Dopo aver aggiunto un gruppo di regole a un ACL Web, le nuove regole del gruppo di regole potrebbero essere in vigore in un'area in cui viene utilizzato l'ACL Web e non in un'altra.
- Dopo aver modificato l'impostazione di un'azione della regola, è possibile vedere la vecchia azione in alcuni punti e la nuova azione in altri.
- Dopo aver aggiunto un indirizzo IP a un set IP utilizzato in una regola di blocco, il nuovo indirizzo potrebbe essere bloccato in un'area mentre è ancora consentito in un'altra.

Gestione del comportamento del gruppo di regole in un'ACL Web

In questa sezione vengono descritte le opzioni per modificare l'utilizzo di un gruppo di regole nell'ACL Web. Queste informazioni si applicano a tutti i tipi di gruppi di regole. Dopo aver aggiunto un gruppo di regole a un ACL Web, è possibile sovrascrivere le azioni delle singole regole del gruppo di regole su Count o su qualsiasi altra impostazione di azione valida. È inoltre possibile sostituire l'azione risultante del gruppo di regole suCount, il che non ha alcun effetto sul modo in cui le regole vengono valutate all'interno del gruppo di regole.

Per informazioni su queste opzioni, consulta Le azioni sostituiscono i gruppi di regole.

Sovrascrivere le azioni delle regole in un gruppo di regole

Per ogni gruppo di regole in un ACL Web, è possibile sovrascrivere le azioni della regola contenuta per alcune o tutte le regole.

Il caso d'uso più comune consiste nell'ignorare le azioni delle regole per Count testare regole nuove o aggiornate. Se hai le metriche abilitate, riceverai le metriche per ogni regola che sostituisci. Per ulteriori informazioni sull'esecuzione di test, consulta Test e ottimizzazione delle protezioni AWS WAF.

Per sovrascrivere le azioni delle regole in un gruppo di regole

È possibile apportare queste modifiche quando si aggiunge un gruppo di regole gestito all'ACL Web e apportarle a qualsiasi tipo di gruppo di regole quando si modifica l'ACL Web. Queste istruzioni si riferiscono a un gruppo di regole che è già stato aggiunto all'ACL web. Ulteriori informazioni su questa opzione sono disponibili all'indirizzoL'azione delle regole ha la precedenza.

1. Modifica l'ACL web.

2. Nella scheda Regole della pagina Web ACL, seleziona il gruppo di regole, quindi scegli Modifica.
3. Nella sezione Regole per il gruppo di regole, gestisci le impostazioni delle azioni in base alle esigenze.

   - Tutte le regole: per impostare un'azione di sostituzione per tutte le regole del gruppo di regole, apri il menu a discesa Sostituisci tutte le azioni delle regole e seleziona l'azione di sostituzione. Per rimuovere le sostituzioni per tutte le regole, seleziona Rimuovi tutte le sostituzioni.
   - Regola singola: per impostare un'azione di sostituzione per una singola regola, apri il menu a discesa della regola e seleziona l'azione di sostituzione. Per rimuovere un'eccezione per una regola, apri il menu a discesa della regola e seleziona Rimuovi override.
4. Quando hai finito di apportare le modifiche, scegli Salva regola. Le impostazioni relative all'azione della regola e all'azione di sostituzione sono elencate nella pagina del gruppo di regole.

L'elenco JSON di esempio seguente mostra una dichiarazione di gruppo di regole all'interno di un ACL web che sostituisce le azioni delle regole con le regole e. Count `CategoryVerifiedSearchEngine` `CategoryVerifiedSocialMedia` In JSON, sovrascrivi tutte le azioni delle regole fornendo una `RuleActionOverrides` voce per ogni singola regola.

```
{
    "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"
   }
}
```

Sovrascrivere il risultato della valutazione di un gruppo di regole con Count

È possibile sovrascrivere l'azione risultante dalla valutazione di un gruppo di regole, senza modificare il modo in cui le regole del gruppo di regole vengono configurate o valutate. Questa opzione non è comunemente utilizzata. Se una regola del gruppo di regole dà luogo a una corrispondenza, questa modifica imposta l'azione risultante dal gruppo di regole aCount.

> **Note**
>
> Si tratta di un caso d'uso non comune. La maggior parte delle modifiche alle azioni viene eseguita a livello di regola, all'interno del gruppo di regole, come descritto in. Sovrascrivere le azioni delle regole in un gruppo di regole

È possibile sovrascrivere l'azione risultante del gruppo di regole nell'ACL Web quando si aggiunge o si modifica il gruppo di regole. Nella console, apri l'azione Ignora gruppo di regole - riquadro opzionale del gruppo di regole e abilita l'override. Nel JSON impostato `OverrideAction` nell'istruzione del gruppo di regole, come mostrato nell'elenco di esempio seguente:

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

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

Associazione o dissociazione di un ACL Web con una risorsa AWS

Puoi utilizzare AWS WAF per creare le seguenti associazioni tra ACLS web e le tue risorse:

- Associa un ACL web regionale a una qualsiasi delle risorse regionali elencate di seguito. Per questa opzione, l'ACL web deve trovarsi nella stessa regione della risorsa.
  - API REST di Amazon API Gateway
  - Application Load Balancer
  - AWS AppSync API GraphQL
  - Bacino d'utenza di Amazon Cognito
  - AWS App Runner servizio
  - AWS istanza Verified Access
- Associa un ACL web globale a una CloudFront distribuzione Amazon. L'ACL web globale avrà una regione codificata degli Stati Uniti orientali (Virginia settentrionale).

È inoltre possibile associare un ACL Web a una CloudFront distribuzione quando si crea o si aggiorna la distribuzione stessa. Per informazioni, consulta Using AWS WAF to Control Access to Your Content nella Amazon CloudFront Developer Guide.

Restrizioni su più associazioni

Puoi associare un singolo ACL web a una o più AWS risorse, in base alle seguenti restrizioni:

- È possibile associare ogni AWS risorsa a un solo ACL web. La relazione tra l'ACL web e AWS le risorse è. one-to-many
- È possibile associare un ACL Web a una o più CloudFront distribuzioni. Non è possibile associare un ACL Web associato a una CloudFront distribuzione a nessun altro AWS tipo di risorsa.

Restrizioni aggiuntive

Le seguenti restrizioni aggiuntive si applicano alle associazioni ACL Web:

- È possibile associare un ACL Web solo a un Application Load Regioni AWS Balancer all'interno. Ad esempio, non è possibile associare un ACL Web a un Application Load Balancer attivo. AWS Outposts
- Non puoi associare un pool di utenti Amazon Cognito a un ACL Web che utilizza il gruppo di regole gestito per la prevenzione delle AWS WAF frodi per la creazione di account Fraud Control (ACFP) `AWSManagedRulesACFPRuleSet` o il gruppo di regole gestito per la prevenzione dell'acquisizione di account AWS WAF Fraud Control (ATP). `AWSManagedRulesATPRuleSet` Per informazioni sulla creazione di account e prevenzione delle frodi, consulta. AWS WAF Fraud Control creazione di account e prevenzione delle frodi (ACFP) Per informazioni sulla prevenzione dell'acquisizione di account, consultaAWS WAF Controllo delle frodi e prevenzione delle acquisizioni di conti (ATP).

> ⚠ Rischio legato al traffico di produzione
>
> Prima di implementare l'ACL Web per il traffico di produzione, testalo e ottimizzalo in un ambiente di staging o di test finché non ti senti a tuo agio con il potenziale impatto sul traffico. Quindi testa e ottimizza le regole in modalità di conteggio con il traffico di produzione prima di attivarle. Per le linee guida, consulta Test e ottimizzazione delle protezioni AWS WAF.

Per associare un ACL Web a una risorsa AWS

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).
3. Scegli il nome dell'ACL web che desideri associare a una risorsa. La console consente di accedere alla descrizione dell'ACL Web, dove è possibile modificarla.
4. Nella scheda AWS Risorse associate, scegli Aggiungi AWS risorse.
5. Quando richiesto, scegli il tipo di risorsa, seleziona il pulsante di opzione accanto alla risorsa che desideri associare, quindi scegli Aggiungi.

Per dissociare un ACL Web da una risorsa AWS

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).

3. Scegliete il nome dell'ACL web che desiderate dissociare dalla risorsa. La console consente di accedere alla descrizione dell'ACL Web, dove è possibile modificarla.
4. Nella scheda AWS Risorse associate, seleziona la risorsa da cui desideri dissociare questo ACL web.

> **Note**
>
> È necessario dissociare una risorsa alla volta. Non scegliere più risorse.

5. Scegli Dissocia. La console apre una finestra di dialogo di conferma. Conferma la tua scelta di dissociare l'ACL Web dalla AWS risorsa.

Eliminazione di un ACL Web

Per eliminare un ACL Web, è innanzitutto necessario dissociare tutte le AWS risorse dall'ACL Web. Esegui la seguente procedura.

Per eliminare un'ACL Web

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).
3. Selezionare il nome dell'ACL Web che si desidera eliminare. La console consente di accedere alla descrizione dell'ACL Web, dove è possibile modificarla.
4. Nella scheda AWS Risorse associate, per ogni risorsa associata, seleziona il pulsante di opzione accanto al nome della risorsa, quindi scegli Dissocia. Questo dissocia l'ACL web dalle tue risorse. AWS
5. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).
6. Selezionare il pulsante di opzione accanto all'ACL Web che si sta eliminando e quindi scegliere Delete (Elimina).

Gruppi di regole

Un gruppo di regole è un insieme riutilizzabile di regole che puoi aggiungere a un'ACL Web. Per ulteriori informazioni sulle ACL Web, consulta Elenchi di controllo degli accessi Web (ACL Web).

I gruppi di regole rientrano nelle seguenti categorie principali:

- I tuoi gruppi di regole, che crei e gestisci.
- Gruppi di regole AWS gestiti che i team di Managed Rules creano e gestiscono per te.
- Gruppi di regole gestiti che Marketplace AWS i venditori creano e gestiscono per te.
- Gruppi di regole posseduti e gestiti da altri servizi come AWS Firewall Manager Shield Advanced.

Differenze tra gruppi di regole e ACL Web

I gruppi di regole e le ACL Web contengono regole, definite nello stesso modo in entrambe le posizioni. I gruppi di regole differiscono dalle ACL Web nei seguenti modi:

- I gruppi di regole non possono contenere istruzioni di riferimento sui gruppi di regole.
- Un singolo gruppo di regole può essere riutilizzato in più ACL Web aggiungendo a ciascuna ACL Web un'istruzione di riferimento del gruppo di regole. Non è possibile riutilizzare un'ACL Web.
- I gruppi di regole non dispongono di operazioni predefinite. In un'ACL Web, viene impostata un'operazione predefinita per ogni regola o gruppo di regole inclusi. Ogni singola regola all'interno di un gruppo di regole o di un'ACL Web dispone di un'operazione definita.
- Non si associa direttamente un gruppo di regole a una AWS risorsa. Per proteggere le risorse utilizzando un gruppo di regole, il gruppo di regole viene utilizzato in un'ACL Web.
- Gli ACL Web hanno una capacità massima definita dal sistema di 5.000 unità di capacità ACL Web (WCU). Ogni gruppo di regole ha un'impostazione WCU che deve essere impostata al momento della creazione. Questa impostazione può essere utilizzata per calcolare i requisiti di capacità aggiuntivi che verrebbero aggiunti all'ACL Web a seguito dell'utilizzo di un gruppo di regole. Per ulteriori informazioni sulle WCU, vedere. AWS WAF unità di capacità Web ACL (WCU)

Per ulteriori informazioni sulle regole, consulta AWS WAF regole.

Questa sezione fornisce indicazioni per la creazione e la gestione dei propri gruppi di regole, descrive i gruppi di regole gestiti disponibili e fornisce indicazioni per l'utilizzo dei gruppi di regole gestiti.

Argomenti

Gruppi di regole gestite

I gruppi di regole gestiti sono raccolte di ready-to-use regole predefinite che AWS Marketplace AWS i venditori scrivono e gestiscono per te. AWS WAF I prezzi di base si applicano all'utilizzo di qualsiasi gruppo di regole gestito. Per informazioni AWS WAF sui prezzi, consulta la sezione AWS WAF Prezzi.

- I gruppi di regole AWS Managed Rules per AWS WAF Bot Control, AWS WAF Fraud Control Account Takeover Prevention (ATP) e AWS WAF Fraud Control per la creazione di account e la prevenzione delle frodi (ACFP) sono disponibili dietro pagamento di costi aggiuntivi, oltre ai costi di base. AWS WAF Per i dettagli sui prezzi, vedere Prezzi di AWS WAF.
- Tutti gli altri gruppi di regole AWS Managed Rules sono disponibili per AWS WAF i clienti senza costi aggiuntivi.
- Marketplace AWS i gruppi di regole gestiti sono disponibili in abbonamento tramite Marketplace AWS. Ciascuno di questi gruppi di regole è di proprietà e gestito dal Marketplace AWS venditore. Per informazioni sui prezzi relativi all'utilizzo di un gruppo di regole Marketplace AWS gestito, contatta il Marketplace AWS venditore.

Alcuni gruppi di regole gestite sono progettati per aiutare a proteggere tipi specifici di applicazioni web come WordPress Joomla o PHP. Altri offrono un'ampia protezione contro le minacce note o le vulnerabilità più comuni delle applicazioni Web, incluse alcune di quelle elencate nella Top 10 di OWASP. Gli utenti soggetti a conformità normativa come PCI e HIPAA, potrebbero essere in grado di usare i gruppi di regole di gestite per soddisfare i requisiti del firewall dell'applicazione Web.

Aggiornamenti automatici

Mantenersi aggiornati sul panorama delle minacce in continua evoluzione può essere dispendioso in termini di tempo e denaro. I gruppi di regole gestiti possono farti risparmiare tempo durante l'implementazione e l'utilizzo. AWS WAF Molti AWS Marketplace AWS venditori aggiornano automaticamente i gruppi di regole gestiti e forniscono nuove versioni dei gruppi di regole quando emergono nuove vulnerabilità e minacce.

In alcuni casi, AWS viene informata delle nuove vulnerabilità prima della divulgazione pubblica, grazie alla sua partecipazione a diverse comunità private di divulgazione. In questi casi, AWS può aggiornare i gruppi di regole AWS Managed Rules e implementarli automaticamente anche prima che una nuova minaccia diventi nota a tutti.

Accesso limitato alle regole in un gruppo di regole gestito

Ogni gruppo di regole gestito fornisce una descrizione completa dei tipi di attacchi e vulnerabilità da cui è progettato per proteggere. Per proteggere la proprietà intellettuale dei fornitori dei gruppi di regole, non è possibile visualizzare tutti i dettagli delle singole regole all'interno di un gruppo di regole. Questa restrizione consente anche di impedire agli utenti malintenzionati di progettare minacce che eludano in modo specifico le regole pubblicate.

Argomenti

Gestione delle versioni con gruppi di regole gestiti

Molti provider di gruppi di regole gestiti aggiornano le opzioni e le funzionalità di un gruppo di regole nelle nuove versioni del gruppo di regole. In genere, una versione specifica di un gruppo di regole gestito è statica. A volte, un provider potrebbe dover aggiornare alcune o tutte le versioni esistenti di un gruppo di regole gestito, ad esempio per rispondere a una minaccia di sicurezza emergente.

Quando aggiungi un gruppo di regole gestito all'ACL Web, se il gruppo di regole supporta il controllo delle versioni, puoi scegliere di consentire al provider di gestire la versione da utilizzare oppure puoi gestire tu stesso l'impostazione della versione.

Non riesci a trovare la versione che desideri?

Se non vedi una versione nell'elenco delle versioni di un gruppo di regole, è probabile che la versione sia prevista per la scadenza o sia già scaduta. Dopo la pianificazione della scadenza di una versione, AWS WAF non ti consente più di sceglierla per il gruppo di regole.

Controllo delle versioni e notifiche SNS per i gruppi di regole AWS Managed Rules

I gruppi di regole AWS Managed Rules forniscono tutti notifiche di controllo delle versioni e di aggiornamento SNS, ad eccezione dei gruppi di regole per la reputazione IP, il controllo dei bot e la prevenzione dell'acquisizione di account.

I gruppi di regole AWS Managed Rules che forniscono le notifiche utilizzano tutti lo stesso argomento SNS Amazon Resource Name (ARN).

Argomenti

Ciclo di vita delle versioni per i gruppi di regole gestiti

I provider gestiscono le seguenti fasi del ciclo di vita di una versione statica di un gruppo di regole gestito:

- Rilascio e aggiornamenti: un provider di gruppi di regole gestiti annuncia le prossime e nuove versioni statiche dei propri gruppi di regole gestiti tramite notifiche a un argomento di Amazon Simple Notification Service (Amazon SNS). I provider potrebbero utilizzare l'argomento anche per comunicare altre informazioni importanti sui propri gruppi di regole, come gli aggiornamenti urgenti richiesti.

  Puoi iscriverti all'argomento del gruppo di regole e configurare come desideri ricevere le notifiche. Per ulteriori informazioni, consulta Ricevere notifiche relative a nuove versioni e aggiornamenti.
- Pianificazione delle scadenze: un fornitore di gruppi di regole gestiti pianifica la scadenza delle versioni precedenti di un gruppo di regole. Una versione con scadenza pianificata non può essere aggiunta alle regole ACL Web. Una volta pianificata la scadenza di una versione, AWS WAF monitora la scadenza con una metrica relativa al conto alla rovescia in Amazon. CloudWatch

  Puoi impostare un allarme sulla metrica CloudWatch per tenere traccia della scadenza di una versione che stai utilizzando. In questo modo hai il tempo di testare una nuova versione e abbandonare quella in scadenza prima del termine del conto alla rovescia. Per ulteriori informazioni, consulta Monitoraggio della scadenza della versione.
- Scadenza della versione: se disponi di un ACL Web configurato per utilizzare una versione scaduta di un gruppo di regole gestito, durante la valutazione dell'ACL Web, AWS WAF utilizza la versione predefinita del gruppo di regole. Inoltre, AWS WAF blocca tutti gli aggiornamenti all'ACL web che non rimuovono il gruppo di regole né ne modificano la versione con una non scaduta.

Se utilizzi gruppi di regole Marketplace AWS gestiti, chiedi al provider eventuali informazioni aggiuntive sui cicli di vita delle versioni.

Procedure consigliate per la gestione delle versioni dei gruppi di regole gestiti

Segui questa guida sulle best practice per la gestione del controllo delle versioni quando utilizzi un gruppo di regole gestito con versioni.

Quando utilizzi un gruppo di regole gestito nell'ACL Web, puoi scegliere di utilizzare una versione statica specifica del gruppo di regole oppure puoi scegliere di utilizzare la versione predefinita:

- Versione predefinita: imposta AWS WAF sempre la versione predefinita sulla versione statica attualmente consigliata dal provider. Quando il provider aggiorna la versione statica consigliata, aggiorna AWS WAF automaticamente l'impostazione della versione predefinita per il gruppo di regole nell'ACL web.

  Quando utilizzi la versione predefinita di un gruppo di regole gestito, procedi come best practice come procedura consigliata:

  - Iscriviti alle notifiche: iscriviti alle notifiche per le modifiche al gruppo di regole e tienile d'occhio. La maggior parte dei provider invia notifiche avanzate sulle nuove versioni statiche e sulle modifiche alle versioni predefinite. Questi consentono di verificare gli effetti di una nuova versione statica prima AWS di passare alla versione predefinita. Per ulteriori informazioni, consulta Ricevere notifiche relative a nuove versioni e aggiornamenti.
  - Esamina gli effetti delle impostazioni della versione statica e apporta le modifiche necessarie prima di impostarla come predefinita. Prima di impostare quella predefinita su una nuova versione statica, esamina gli effetti della versione statica sul monitoraggio e la gestione delle tue richieste web. La nuova versione statica potrebbe avere nuove regole da rivedere. Cerca falsi positivi o altri comportamenti imprevisti, nel caso in cui sia necessario modificare il modo in cui utilizzi il gruppo di regole. Puoi impostare regole di conteggio, ad esempio, per impedire che blocchino il traffico mentre cerchi di capire come gestire il nuovo comportamento. Per ulteriori informazioni, consulta Test e ottimizzazione delle protezioni AWS WAF.
- Versione statica: se scegli di utilizzare una versione statica, devi aggiornare manualmente l'impostazione della versione quando sei pronto per adottare una nuova versione del gruppo di regole.

  Quando utilizzi una versione statica di un gruppo di regole gestito, segui le seguenti procedure consigliate:

  - Mantieni la tua versione aggiornata: mantieni il tuo gruppo di regole gestito il più vicino possibile alla versione più recente. Quando viene rilasciata una nuova versione, testala, modifica le impostazioni in base alle esigenze e implementala tempestivamente. Per informazioni sui test, consultaTest e ottimizzazione delle protezioni AWS WAF.
  - Iscriviti alle notifiche: iscriviti alle notifiche per le modifiche al gruppo di regole, in modo da sapere quando il tuo provider rilascia nuove versioni statiche. La maggior parte dei provider fornisce notifiche avanzate sulle modifiche alle versioni. Inoltre, il tuo provider potrebbe dover aggiornare

la versione statica che stai utilizzando per colmare una falla di sicurezza o per altri motivi urgenti. Saprai cosa sta succedendo se sei abbonato alle notifiche del provider. Per ulteriori informazioni, consulta Ricevere notifiche relative a nuove versioni e aggiornamenti.

- Evita la scadenza della versione: non lasciare scadere una versione statica mentre la usi. La gestione delle versioni scadute da parte del provider può variare e potrebbe includere l'imposizione di un aggiornamento a una versione disponibile o altre modifiche che possono avere conseguenze impreviste. Tieni traccia della metrica di AWS WAF scadenza e imposta un allarme che ti dia un numero di giorni sufficiente per eseguire correttamente l'aggiornamento a una versione supportata. Per ulteriori informazioni, consulta Monitoraggio della scadenza della versione.

Utilizzo di gruppi di regole gestite

Questa sezione fornisce indicazioni per l'accesso e la gestione dei gruppi di regole gestiti.

Quando aggiungi un gruppo di regole gestito all'ACL Web, puoi scegliere le stesse opzioni di configurazione dei tuoi gruppi di regole, oltre a impostazioni aggiuntive.

Tramite la console, è possibile accedere alle informazioni sui gruppi di regole gestiti durante il processo di aggiunta e modifica delle regole negli ACL Web. Tramite le API e l'interfaccia a riga di comando (CLI), puoi richiedere direttamente informazioni sui gruppi di regole gestiti.

Quando utilizzi un gruppo di regole gestito nell'ACL Web, puoi modificare le seguenti impostazioni:

- Versione: è disponibile solo se il gruppo di regole dispone di una versione. Per ulteriori informazioni, consulta Gestione delle versioni con gruppi di regole gestiti.
- Sostituisci le azioni delle regole: è possibile sostituire le azioni per le regole del gruppo di regole con qualsiasi azione. La loro impostazione Count è utile per testare un gruppo di regole prima di utilizzarlo per gestire le richieste Web. Per ulteriori informazioni, consulta L'azione delle regole ha la precedenza.
- Istruzione Scope-down: puoi aggiungere un'istruzione scope-down per filtrare le richieste Web che non desideri valutare con il gruppo di regole. Per ulteriori informazioni, consulta Dichiarazioni delimitate.
- Ignora l'azione del gruppo di regole: puoi ignorare l'azione risultante dalla valutazione del gruppo di regole e impostarla su only. Count Questa opzione non è comunemente utilizzata. Non altera il modo in cui AWS WAF valuta le regole nel gruppo di regole. Per ulteriori informazioni, consulta L'azione di gruppo di regole viene sostituita da Count.

Per modificare le impostazioni del gruppo di regole gestito nell'ACL Web

- Console
  - (Opzione) Quando aggiungi il gruppo di regole gestite all'ACL web, puoi scegliere Modifica per visualizzare e modificare le impostazioni.
  - (Opzione) Dopo aver aggiunto il gruppo di regole gestito all'ACL Web, dalla pagina Web ACL, scegli l'ACL Web appena creato. Questo consente di passare alla pagina di modifica dell'ACL Web.
    - Seleziona Rules (Regole).
    - Seleziona il gruppo di regole, quindi scegli Modifica per visualizzare e modificare le impostazioni.
- API e CLI: al di fuori della console, puoi gestire le impostazioni del gruppo di regole gestito quando crei e aggiorni l'ACL Web.

Recupero dell'elenco dei gruppi di regole gestiti

È possibile recuperare l'elenco dei gruppi di regole gestiti disponibili per l'uso negli ACL Web. L'elenco include quanto segue:

- Tutti i gruppi di regole AWS Managed Rules.
- I gruppi di Marketplace AWS regole a cui ti sei iscritto.

> **Note**
>
> Per informazioni sulla sottoscrizione ai gruppi di Marketplace AWS regole, vedere. Marketplace AWS gruppi di regole gestiti

Quando recuperi l'elenco dei gruppi di regole gestiti, l'elenco che ottieni dipende dall'interfaccia che stai utilizzando:

- Console: tramite la console, puoi vedere tutti i gruppi di regole gestiti, inclusi i gruppi di Marketplace AWS regole a cui non sei ancora abbonato. Per quelli a cui non sei ancora abbonato, l'interfaccia fornisce dei link che puoi seguire per iscriverti.
- API e CLI: al di fuori della console, la richiesta restituisce solo i gruppi di regole disponibili per l'uso.

Per recuperare l'elenco dei gruppi di regole gestiti

- Console: durante il processo di creazione di un ACL Web, nella pagina Aggiungi regole e gruppi di regole, scegli Aggiungi gruppi di regole gestiti. Al livello più alto, sono elencati i nomi dei provider. Espandi l'elenco di ogni provider per visualizzare l'elenco dei gruppi di regole gestiti. Per i gruppi di regole con versione, le informazioni mostrate a questo livello si riferiscono alla versione predefinita. Quando si aggiunge un gruppo di regole gestite all'ACL Web, viene elencato dalla console in base allo schema di denominazione `<Vendor Name>-<Managed Rule Group Name>`.
- API:
  - `ListAvailableManagedRuleGroups`
- CLI —
  - `aws wafv2 list-available-managed-rule-groups --scope=<CLOUDFRONT|REGIONAL>`

Recupero delle regole in un gruppo di regole gestito

È possibile recuperare un elenco delle regole in un gruppo di regole gestito. Le chiamate API e CLI restituiscono le specifiche delle regole a cui puoi fare riferimento nel modello JSON o tramite. AWS CloudFormation

Per recuperare l'elenco di regole in un gruppo di regole gestite

- Console
  - (Opzione) Quando aggiungi il gruppo di regole gestite all'ACL Web, puoi scegliere Modifica per visualizzare le regole.
  - (Opzione) Dopo aver aggiunto il gruppo di regole gestite all'ACL Web, dalla pagina Web ACL, scegli l'ACL Web appena creato. Questo consente di passare alla pagina di modifica dell'ACL Web.
    - Seleziona Rules (Regole).
    - Seleziona il gruppo di regole per cui desideri visualizzare un elenco di regole, quindi scegli Modifica. AWS WAF mostra l'elenco delle regole nel gruppo di regole.
- API: `DescribeManagedRuleGroup`
- CLI — `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Recupero delle versioni disponibili per un gruppo di regole gestito

Le versioni disponibili di un gruppo di regole gestito sono versioni la cui scadenza non è ancora stata programmata. L'elenco indica quale versione è la versione predefinita corrente per il gruppo di regole.

Per recuperare un elenco delle versioni disponibili di un gruppo di regole gestito

- Console
  - (Opzione) Quando aggiungi il gruppo di regole gestito all'ACL Web, scegli Modifica per visualizzare le informazioni sul gruppo di regole. Espandi il menu a discesa Versione per visualizzare l'elenco delle versioni disponibili.
  - (Opzione) Dopo aver aggiunto il gruppo di regole gestito all'ACL Web, scegli Modifica nell'ACL Web, quindi seleziona e modifica la regola del gruppo di regole. Espandi il menu a discesa Versione per visualizzare l'elenco delle versioni disponibili.
- API:
  - `ListAvailableManagedRuleGroupVersions`
- CLI —
  - `aws wafv2 list-available-managed-rule-group-versions --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Aggiungere un gruppo di regole gestito a un ACL Web tramite la console

Questa guida si applica a tutti i gruppi di regole AWS Managed Rules e ai gruppi di Marketplace AWS regole a cui sei iscritto.

> **Rischio legato al traffico di produzione**
>
> Prima di implementare modifiche all'ACL Web per il traffico di produzione, testale e ottimizzale in un ambiente di staging o di test finché non ti rendi conto del potenziale impatto sul traffico. Quindi testa e ottimizza le regole aggiornate in modalità di conteggio con il traffico di produzione prima di attivarle. Per le linee guida, consulta Test e ottimizzazione delle protezioni AWS WAF.

> **Note**
>
> L'utilizzo di più di 1.500 WCU in un ACL Web comporta costi superiori al prezzo base dell'ACL Web. Per ulteriori informazioni, consulta AWS WAF unità di capacità Web ACL (WCU) e Prezzi di AWS WAF.

Per aggiungere un gruppo di regole gestito a un ACL Web tramite la console

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Scegli Web ACL nel riquadro di navigazione.
3. Nella pagina Web ACL, dall'elenco degli ACL Web, seleziona quello a cui desideri aggiungere il gruppo di regole. Verrà visualizzata la pagina relativa al singolo ACL Web.
4. Nella pagina dell'ACL web, scegli la scheda Regole.
5. Nel riquadro Regole, scegli Aggiungi regole, quindi scegli Aggiungi gruppi di regole gestiti.
6. Nella pagina Aggiungi gruppi di regole gestiti, espandi la selezione del fornitore del tuo gruppo di regole per visualizzare l'elenco dei gruppi di regole disponibili.
7. Per ogni gruppo di regole che desideri aggiungere, scegli Aggiungi a ACL web. Se desideri modificare la configurazione dell'ACL Web per il gruppo di regole, scegli Modifica, apporta le modifiche e quindi scegli Salva regola. Per informazioni sulle opzioni, consulta la guida al controllo delle versioni all'indirizzo Gestione delle versioni con gruppi di regole gestiti e la guida per l'utilizzo di un gruppo di regole gestito in un ACL Web all'indirizzo. Istruzione gruppo di regole gestite
8. Nella parte inferiore della pagina Aggiungi gruppi di regole gestiti, scegli Aggiungi regole.
9. Nella pagina Imposta la priorità delle regole, modifica l'ordine in cui le regole vengono eseguite secondo necessità, quindi scegli Salva. Per ulteriori informazioni, consulta Ordine di elaborazione delle regole e dei gruppi di regole in un ACL Web.

Nella pagina Web ACL, i gruppi di regole gestiti che hai aggiunto sono elencati nella scheda Regole.

Testa e ottimizza eventuali modifiche alle tue AWS WAF protezioni prima di utilizzarle per il traffico di produzione. Per informazioni, consulta Test e ottimizzazione delle protezioni AWS WAF.

Incoerenze temporanee durante gli aggiornamenti

Quando si crea o si modifica un ACL Web o altre AWS WAF risorse, le modifiche richiedono poco tempo per essere propagate in tutte le aree in cui sono archiviate le risorse. Il tempo di propagazione può variare da pochi secondi a diversi minuti.

Di seguito sono riportati alcuni esempi delle incongruenze temporanee che potreste notare durante la propagazione delle modifiche:

- Dopo aver creato un ACL Web, se provi ad associarlo a una risorsa, potresti ricevere un'eccezione che indica che l'ACL Web non è disponibile.
- Dopo aver aggiunto un gruppo di regole a un ACL Web, le nuove regole del gruppo di regole potrebbero essere in vigore in un'area in cui viene utilizzato l'ACL Web e non in un'altra.
- Dopo aver modificato l'impostazione di un'azione della regola, è possibile vedere la vecchia azione in alcuni punti e la nuova azione in altri.
- Dopo aver aggiunto un indirizzo IP a un set IP utilizzato in una regola di blocco, il nuovo indirizzo potrebbe essere bloccato in un'area mentre è ancora consentito in un'altra.

Ricevere notifiche sulle nuove versioni e sugli aggiornamenti di un gruppo di regole gestito

Un provider di gruppi di regole gestiti utilizza le notifiche SNS per annunciare le modifiche ai gruppi di regole, come nuove versioni imminenti e aggiornamenti di sicurezza urgenti.

Come abbonarsi alle notifiche SNS

Per iscriverti alle notifiche per un gruppo di regole, crei un abbonamento Amazon SNS per l'argomento Amazon SNS del gruppo di regole ARN nella regione Stati Uniti orientali (Virginia settentrionale) us-east-1.

Per informazioni su come abbonarsi, consulta la Amazon Simple Notification Service Developer Guide.

> **Note**
>
> Crea il tuo abbonamento per l'argomento SNS solo nella regione us-east-1.

Dove trovare l'ARN dell'argomento Amazon SNS per un gruppo di regole gestito

AWS I gruppi di regole Managed Rules utilizzano un unico ARN di argomenti SNS, quindi è possibile recuperare l'ARN dell'argomento da uno dei gruppi di regole e sottoscriverlo per ricevere notifiche per tutti i gruppi di regole Managed Rules che AWS forniscono notifiche SNS.

- Console
  - (Opzione) Quando aggiungi il gruppo di regole gestito all'ACL Web, scegli Modifica per visualizzare le informazioni sul gruppo di regole, che include l'argomento ARN di Amazon SNS del gruppo di regole.
  - (Opzione) Dopo aver aggiunto il gruppo di regole gestito all'ACL Web, scegli Modifica nell'ACL Web, quindi seleziona e modifica la regola del gruppo di regole per visualizzare l'argomento ARN dell'argomento Amazon SNS del gruppo di regole.
- API: `DescribeManagedRuleGroup`
- CLI — `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Controllo delle versioni e notifiche SNS per i gruppi di regole AWS Managed Rules

I gruppi di regole AWS Managed Rules forniscono tutti notifiche di controllo delle versioni e di aggiornamento SNS, ad eccezione dei gruppi di regole per la reputazione IP, il controllo dei bot e la prevenzione dell'acquisizione di account.

I gruppi di regole AWS Managed Rules che forniscono le notifiche utilizzano tutti lo stesso argomento SNS Amazon Resource Name (ARN).

Per le distribuzioni che influiscono sulle protezioni, come le modifiche alla versione predefinita, AWS fornisce notifiche SNS per informarti delle distribuzioni pianificate e per farti sapere quando inizia una distribuzione. Per le distribuzioni che non influiscono sulle protezioni, come le distribuzioni con release candidate e versioni statiche, AWS potrebbe inviarti una notifica dopo l'inizio della distribuzione o anche dopo il suo completamento. Al termine della distribuzione di una nuova versione statica, AWS aggiorna questa guida, nel changelog all'indirizzo AWS Registro delle modifiche di Managed Rules e nella pagina della cronologia dei documenti all'indirizzo. Cronologia dei documenti Per ulteriori informazioni sulle notifiche fornite per ogni tipo di distribuzione, vedere. Distribuzioni per gruppi di regole AWS Managed Rules con versioni

Per ricevere tutti gli aggiornamenti relativi AWS ai gruppi di regole AWS Managed Rules, iscriviti al feed RSS da qualsiasi pagina HTML di questa guida e iscriviti all'argomento SNS relativo ai gruppi di regole AWS Managed Rules.

I campi nelle notifiche di Amazon SNS includono sempre Oggetto, Messaggio e. MessageAttributes I campi aggiuntivi dipendono dal tipo di messaggio e dal gruppo di regole gestite a cui è destinata la notifica. Di seguito viene mostrato un esempio di elenco di notifiche per`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"
        }
    }
}
```

Per informazioni generali sui formati di notifica di Amazon SNS e su come filtrare le notifiche che ricevi, consulta Parsing message formats e policy di filtro degli abbonamenti Amazon SNS nella Amazon Simple Notification Service Developer Guide.

Monitoraggio della scadenza della versione di un gruppo di regole

Se utilizzi una versione specifica di un gruppo di regole, assicurati di non continuare a utilizzare una versione dopo la data di scadenza.

> **Tip**
>
> Se tieni traccia delle modifiche imminenti per il gruppo di regole gestito tramite Amazon SNS, riceverai notifiche sulle versioni nuove e consigliate. Se esegui regolarmente test e passi a una versione più recente, sarai sempre aggiornato sulle attività relative alla scadenza delle versioni precedenti. Potrai inoltre beneficiare delle protezioni più recenti previste dal gruppo di regole. Per informazioni sulle notifiche, consultaRicevere notifiche relative a nuove versioni e aggiornamenti.

Se una versione che stai utilizzando è scaduta, AWS WAF blocca le modifiche all'ACL web in cui utilizzi il gruppo di regole. Il blocco rimane valido finché non aggiorni il gruppo di regole a una versione disponibile o lo rimuovi dall'ACL web.

La gestione delle scadenze per un gruppo di regole gestito dipende dal fornitore del gruppo di regole. Per i gruppi di regole AWS Managed Rules, la versione viene automaticamente modificata nella versione predefinita del gruppo di regole. Per i gruppi di Marketplace AWS regole, chiedi al provider come gestiscono la scadenza.

Per monitorare la pianificazione delle scadenze per un gruppo di regole gestito, monitora i parametri di CloudWatch scadenza di Amazon da: AWS WAF

- Nome parametro: DaysToExpiry
- Dimensioni metriche:Region,, e ManagedRuleGroup Vendor Version

Individua la metrica per il tuo gruppo di regole gestito in Amazon CloudWatch e imposta un allarme in modo da ricevere una notifica in tempo utile per passare a una versione più recente del tuo gruppo di regole. Per informazioni sull'uso dei CloudWatch parametri di Amazon e sulla configurazione degli allarmi, consulta la Amazon CloudWatch User Guide.

Quando il provider crea una nuova versione del gruppo di regole, imposta la durata prevista della versione. Sebbene la scadenza della versione non sia pianificata, il valore della metrica è impostato sull'impostazione della durata prevista e, all'interno CloudWatch, vedrai un valore fisso per la metrica.

Dopo che il provider ha pianificato la scadenza della metrica, il valore della metrica diminuisce ogni giorno fino a raggiungere lo zero il giorno della scadenza.

Se disponi di un gruppo di regole gestito nell'ACL Web che valuta il traffico, otterrai una metrica corrispondente. La metrica non è disponibile per i gruppi di regole non utilizzati.

Esempi di configurazioni gestite di gruppi di regole in JSON e YAML

Le chiamate API e CLI restituiscono un elenco di tutte le regole del gruppo di regole gestito a cui puoi fare riferimento nel modello JSON o tramite. AWS CloudFormation

JSON

Puoi fare riferimento e modificare i gruppi di regole gestite all'interno di un'istruzione regola utilizzando JSON. L'elenco seguente mostra il gruppo di regole AWS Managed Rules`AWSManagedRulesCommonRuleSet`, in formato JSON. La RuleActionOverrides specifica elenca una regola la cui azione è stata sostituita. 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

È possibile fare riferimento e modificare i gruppi di regole gestiti all'interno di un'istruzione di regole utilizzando il modello AWS CloudFormation YAML. L'elenco seguente mostra il gruppo di regole AWS Managed Rules`AWSManagedRulesCommonRuleSet`, nel AWS CloudFormation modello. La RuleActionOverrides specifica elenca una regola la cui azione è stata sostituita. 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 Regole gestite per AWS WAF

AWS Managed Rules for AWS WAF è un servizio gestito che fornisce protezione dalle vulnerabilità comuni delle applicazioni o da altro traffico indesiderato. È possibile selezionare uno o più gruppi di regole da AWS Managed Rules per ogni ACL Web, fino al limite massimo di unità di capacità Web ACL (WCU).

Mitigazione dei falsi positivi e test delle modifiche ai gruppi di regole

Prima di utilizzare qualsiasi gruppo di regole gestito in produzione, testalo in un ambiente non di produzione secondo le indicazioni riportate in. Test e ottimizzazione delle protezioni AWS WAF Segui le indicazioni relative al test e all'ottimizzazione quando aggiungi un gruppo di regole all'ACL Web, per testare una nuova versione di un gruppo di regole e ogni volta che un gruppo di regole non gestisce il traffico web nel modo desiderato.

Responsabilità di sicurezza condivise

AWS Le Managed Rules sono progettate per proteggerti dalle minacce web più comuni. Se utilizzati in conformità con la documentazione, i gruppi di regole AWS Managed Rules aggiungono un altro livello di sicurezza per le applicazioni. Tuttavia, i gruppi di regole AWS Managed Rules non sono intesi come sostituti delle responsabilità in materia di sicurezza, che sono determinate dalle AWS risorse selezionate. Fai riferimento al modello di responsabilità condivisa per assicurarti che le tue risorse AWS siano adeguatamente protette.

AWS Elenco dei gruppi di regole di Managed Rules

Le informazioni che pubblichiamo per le regole nei gruppi di regole AWS Managed Rules hanno lo scopo di fornirti informazioni sufficienti per utilizzare le regole, senza fornire informazioni che i malintenzionati potrebbero utilizzare per aggirarle. Se hai bisogno di più informazioni di quelle che trovi in questa documentazione, contatta il AWS Support Centro.

Questa sezione descrive le versioni più recenti dei gruppi di regole AWS Managed Rules. Vengono visualizzati nella console quando aggiungi un gruppo di regole gestite all'ACL Web. Tramite l'API, puoi recuperare questo elenco insieme ai gruppi di regole Marketplace AWS gestite a cui sei abbonato chiamando. `ListAvailableManagedRuleGroups`

> **Note**
>
> Per informazioni sul recupero delle versioni di un gruppo di regole AWS Managed Rules, consulta. Recupero delle versioni disponibili per un gruppo di regole gestito

Tutti i gruppi di regole AWS Managed Rules supportano l'etichettatura e gli elenchi di regole in questa sezione includono le specifiche delle etichette. È possibile recuperare le etichette per un gruppo di regole gestito tramite l'API chiamando. `DescribeManagedRuleGroup` Le etichette sono elencate nella AvailableLabels proprietà nella risposta. Per informazioni sull'etichettatura, vedereAWS WAF etichette sulle richieste web.

Testa e ottimizza eventuali modifiche alle tue AWS WAF protezioni prima di utilizzarle per il traffico di produzione. Per informazioni, consulta Test e ottimizzazione delle protezioni AWS WAF.

AWS Gruppi di regole gestite

- Gruppi di regole di base
  - Gruppo di regole gestito dal Core Rule Set (CRS)
  - Gruppo di regole gestito per la protezione degli amministratori
  - Input non validi noti: gruppo di regole gestito
- Gruppi di regole specifici del caso d'uso
  - Gruppo di regole gestito dal database SQL
  - Gruppo di regole gestito dal sistema operativo Linux
  - gruppo di regole gestito dal sistema operativo POSIX
  - Gruppo di regole gestito dal sistema operativo Windows
  - Gruppo di regole gestito dall'applicazione PHP
  - WordPress gruppo di regole gestito dall'applicazione
- Gruppi di regole Reputazione IP
  - Gruppo di regole gestito con Amazon IP Reputation List
  - Gruppo di regole gestito con elenco IP anonimo
- AWS WAF Gruppo di regole per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control
  - Utilizzo di questo gruppo di regole
  - Etichette aggiunte da questo gruppo di regole
    - Etichette con token
    - Etichette ACFP
  - Elenco delle regole di prevenzione delle frodi per la creazione di account
- AWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi
  - Utilizzo di questo gruppo di regole
  - Etichette aggiunte da questo gruppo di regole
    - Etichette con token
    - Etichette ATP
  - Elenco delle regole di prevenzione dell'acquisizione di account

- AWS WAF Gruppo di regole Bot Control
  - Livelli di protezione
  - Utilizzo di questo gruppo di regole
  - Etichette aggiunte da questo gruppo di regole
    - Etichette con token
    - Etichette Bot Control
  - Elenco delle regole di Bot Control

Gruppi di regole di base

I gruppi di regole gestite di base forniscono una protezione generale contro una vasta gamma di minacce comuni. Scegli uno o più di questi gruppi di regole per stabilire la protezione di base per le risorse.

> **Note**
>
> Le informazioni che pubblichiamo per le regole nei gruppi di regole AWS Managed Rules hanno lo scopo di fornirti informazioni sufficienti per utilizzare le regole, senza fornire informazioni che i malintenzionati potrebbero utilizzare per aggirarle. Se hai bisogno di più informazioni di quelle che trovi in questa documentazione, contatta il AWS Support Centro.

Gruppo di regole gestito dal Core Rule Set (CRS)

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

Il gruppo di regole di base (CRS) contiene regole generalmente applicabili alle applicazioni Web. Ciò fornisce protezione contro lo sfruttamento di un'ampia gamma di vulnerabilità, incluse alcune delle vulnerabilità ad alto rischio e più comuni descritte nelle pubblicazioni OWASP come OWASP Top 10. Prendi in considerazione l'utilizzo di questo gruppo di regole per qualsiasi caso d'uso. AWS WAF

Questo gruppo di regole gestito aggiunge etichette alle richieste Web che valuta, che sono disponibili per le regole che seguono questo gruppo di regole nell'ACL Web. AWS WAF registra anche le etichette in base ai CloudWatch parametri di Amazon. Per informazioni generali sulle etichette e sui parametri delle etichette, consulta Etichette sulle richieste web e. Metriche e dimensioni delle etichette

> **Note**
>
> Questa tabella descrive l'ultima versione statica di questo gruppo di regole. Per le altre versioni, utilizzare il comando API DescribeManagedRuleGroup.

Nome regola	Descrizione ed etichetta
`NoUserAgent_HEADER`	Verifica la presenza di richieste prive dell'`User-Agent` intestazione HTTP. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:NoUserAgent_Header`
`UserAgent_BadBots_HEADER`	Verifica la presenza di valori di `User-Agent` intestazione comuni che indicano che la richiesta è un bot errato. I modelli di esempio includono `nessus` e `nmap`. Per la gestione dei bot, vedi anche. AWS WAF Gruppo di regole Bot Control Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:BadBots_Header`
`SizeRestrictions_QUERYSTRING`	Controlla le stringhe di query URI che superano i 2.048 byte. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:SizeRestrictions_QueryString`

Nome regola	Descrizione ed etichetta
`SizeRestrictions_Cookie_HEADER`	Controlla le intestazioni dei cookie che superano i 10.240 byte. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:SizeRestrictions_Cookie_Header`
`SizeRestrictions_BODY`	Verifica la presenza di corpi di richiesta di dimensioni superiori a 8 KB (8.192 byte). Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:SizeRestrictions_Body`
`SizeRestrictions_URIPATH`	Controlla i percorsi URI che superano i 1.024 byte. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:SizeRestrictions_URIPath`

Nome regola	Descrizione ed etichetta
`EC2MetaDataSSRF_BODY`	Esamina i tentativi di esfiltrare i metadati di Amazon EC2 dal corpo della richiesta. **Warning** Questa regola ispeziona il corpo della richiesta solo fino al limite di dimensione del corpo per l'ACL Web e il tipo di risorsa. Per Application Load Balancer and AWS AppSync, il limite è fissato a 8 KB. Per CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, il limite predefinito è 16 KB e puoi aumentare il limite fino a 64 KB nella configurazione ACL web. Questa regola utilizza l'`Continue`opzione per la gestione di contenuti di grandi dimensioni. Per ulteriori informazioni, consulta Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Body`

Nome regola	Descrizione ed etichetta
`EC2MetaDataSSRF_COOKIE`	Esamina i tentativi di esfiltrare i metadati di Amazon EC2 dal cookie di richiesta. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Cookie`
`EC2MetaDataSSRF_URIPATH`	Esamina i tentativi di esfiltrare i metadati di Amazon EC2 dal percorso URI della richiesta. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_URIPath`
`EC2MetaDataSSRF_QUERYARGUMENTS`	Esamina i tentativi di esfiltrare i metadati di Amazon EC2 dagli argomenti della query della richiesta. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_QueryArguments`

Nome regola	Descrizione ed etichetta
`GenericLFI_QUERYARGUMENTS`	Controlla la presenza di exploit LFI (Local File Inclusion) negli argomenti della query. Gli esempi includono tentativi di path traversal utilizzando tecniche come `../../`. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:GenericLFI_QueryArguments`
`GenericLFI_URIPATH`	Controlla la presenza di exploit LFI (Local File Inclusion) nel percorso URI. Gli esempi includono tentativi di path traversal utilizzando tecniche come `../../`. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:GenericLFI_URIPath`

Nome regola	Descrizione ed etichetta
`GenericLFI_BODY`	Controlla la presenza di exploit LFI (Local File Inclusion) nel corpo della richiesta. Gli esempi includono tentativi di path traversal utilizzando tecniche come `../../`. **Warning** Questa regola controlla solo il corpo della richiesta fino al limite di dimension e del corpo per l'ACL Web e il tipo di risorsa. Per Application Load Balancer and AWS AppSync, il limite è fissato a 8 KB. Per CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, il limite predefinito è 16 KB e puoi aumentare il limite fino a 64 KB nella configurazione ACL web. Questa regola utilizza l'`Continue`opzione per la gestione di contenuti di grandi dimensioni. Per ulteriori informazioni, consulta Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:GenericLFI_Body`

Nome regola	Descrizione ed etichetta
`RestrictedExtensions_URIPATH`	Controlla le richieste i cui percorsi URI contengono estensioni di file di sistema che non sono sicure da leggere o eseguire. I modelli di esempio includono estensioni quali `.log` e `.ini`. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:RestrictedExtensions_URIPath`
`RestrictedExtensions_QUERYARGUMENTS`	Controlla le richieste i cui argomenti di interrogazione contengono estensioni di file di sistema che non sono sicure da leggere o eseguire. I modelli di esempio includono estensioni quali `.log` e `.ini`. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:RestrictedExtensions_QueryArguments`

Nome regola	Descrizione ed etichetta
`GenericRFI_QUERYARGUMENTS`	Controlla i valori di tutti i parametri di query per rilevare eventuali tentativi di sfruttare la RFI (Remote File Inclusion) nelle applicazioni Web incorporando URL che contengono indirizzi IPv4. Gli esempi includono modelli come `http://`, `https://`, `ftp://` e `ftps://`, con un'intestazione host `file://` IPv4 nel tentativo di exploit. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:GenericRFI_QueryArguments`

Nome regola	Descrizione ed etichetta
`GenericRFI_BODY`	Ispeziona il corpo della richiesta per rilevare eventuali tentativi di sfruttare la RFI (Remote File Inclusion) nelle applicazioni Web incorporando URL che contengono indirizzi IPv4. Gli esempi includono modelli come`http://`,,, e `https://` `ftp://``ftps://`, con un'intestazione host `file://` IPv4 nel tentativo di exploit. **Warning** Questa regola controlla solo il corpo della richiesta fino al limite di dimensione del corpo per l'ACL Web e il tipo di risorsa. Per Application Load Balancer and AWS AppSync, il limite è fissato a 8 KB. Per CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, il limite predefinito è 16 KB e puoi aumentare il limite fino a 64 KB nella configurazione ACL web. Questa regola utilizza l'`Continue`opzione per la gestione di contenuti di grandi dimensioni. Per ulteriori informazioni, consulta Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:GenericRFI_Body`

Nome regola	Descrizione ed etichetta
`GenericRFI_URIPATH`	Ispeziona il percorso URI per individuare eventuali tentativi di sfruttare l'RFI (Remote File Inclusion) nelle applicazioni Web incorporando URL che contengono indirizzi IPv4. Gli esempi includono modelli come`http://`,,, e `https://` `ftp://``ftps://`, con un'intestazione host `file://` IPv4 nel tentativo di exploit.  Operazione delle regole: Block  Etichetta: `awswaf:managed:aws:core-rule-set:GenericRFI_URIPath`

Nome regola	Descrizione ed etichetta
`CrossSiteScripting_COOKIE`	Controlla i valori delle intestazioni dei cookie per individuare i modelli XSS (Common Cross-Site Scripting) utilizzando la funzionalità integrata. AWS WAF Istruzione regola di attacco di Cross-site scripting I modelli di esempio includono script come `<script>alert("hello")</script>` . **Note** I dettagli sulla corrispondenza delle regole nei AWS WAF log non sono compilati per la versione 2.0 di questo gruppo di regole. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_Cookie`

Nome regola	Descrizione ed etichetta
`CrossSiteScripting_QUERYARGUMENTS`	Controlla i valori degli argomenti di interrogazione per i modelli XSS (Common Cross-Site Scripting) utilizzando la funzionalità integrata. AWS WAF Istruzione regola di attacco di Cross-site scripting I modelli di esempio includono script come `<script>alert("hello")</script>` . **Note** I dettagli sulla corrispondenza delle regole nei AWS WAF log non sono compilati per la versione 2.0 di questo gruppo di regole. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_QueryArguments`

Nome regola	Descrizione ed etichetta
`CrossSiteScripting_BODY`	Ispeziona il corpo della richiesta alla ricerca di modelli XSS (Common Cross-Site Scripting) utilizzando la funzionalità integrata. AWS WAF Istruzione regola di attacco di Cross-site scripting I modelli di esempio includono script come `<script>alert("hello")</script>` . **Note** I dettagli sulla corrispondenza delle regole nei AWS WAF log non sono compilati per la versione 2.0 di questo gruppo di regole. **Warning** Questa regola controlla solo il corpo della richiesta fino al limite di dimension e del corpo per l'ACL Web e il tipo di risorsa. Per Application Load Balancer and AWS AppSync, il limite è fissato a 8 KB. Per CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, il limite predefinito è 16 KB e puoi aumentare il limite fino a 64 KB nella configurazione ACL web. Questa regola utilizza l'`Continue`opzione per la gestione di contenuti di grandi dimensioni. Per ulteriori informazioni, consulta Gestione

Nome regola	Descrizione ed etichetta
	di componenti di richieste Web di grandi dimensioni in AWS WAF. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_Body`
`CrossSiteScripting_URIPATH`	Controlla il valore del percorso URI per i modelli XSS (Common Cross-Site Scripting) utilizzando la funzionalità integrata. AWS WAF Istruzione regola di attacco di Cross-site scripting I modelli di esempio includono script come `<script>alert("hello")</script>` . **Note** I dettagli sulla corrispondenza delle regole nei AWS WAF log non sono compilati per la versione 2.0 di questo gruppo di regole. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_URIPath`

Gruppo di regole gestito per la protezione degli amministratori

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

Il gruppo di regole Admin protection contiene regole che consentono di bloccare l'accesso esterno alle pagine amministrative esposte. Ciò potrebbe essere utile se esegui software di terza parte o se desideri ridurre il rischio che un utente malintenzionato ottenga l'accesso amministrativo all'applicazione.

Questo gruppo di regole gestito aggiunge etichette alle richieste Web che valuta, che sono disponibili per le regole che seguono questo gruppo di regole nell'ACL Web. AWS WAF registra anche le etichette in base ai CloudWatch parametri di Amazon. Per informazioni generali sulle etichette e sui parametri delle etichette, consulta Etichette sulle richieste web e. Metriche e dimensioni delle etichette

> **Note**
>
> Questa tabella descrive l'ultima versione statica di questo gruppo di regole. Per le altre versioni, utilizzare il comando API DescribeManagedRuleGroup.

Nome regola	Descrizione ed etichetta
`AdminProtection_URIPATH`	Controlla i percorsi URI che sono generalme nte riservati all'amministrazione di un server Web o di un'applicazione. I modelli di esempio includono `sqlmanager` . Operazione delle regole: Block Etichetta: `awswaf:managed:aws:admin-protection:AdminProtection_URIPath`

Input non validi noti: gruppo di regole gestito

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

Il gruppo di regole Known bad inputs contiene regole per bloccare i modelli di richiesta noti per essere non validi e associati allo sfruttamento o all'individuazione di vulnerabilità. Ciò può contribuire a ridurre il rischio che un utente malintenzionato scopra un'applicazione vulnerabile.

Questo gruppo di regole gestito aggiunge etichette alle richieste Web che valuta, che sono disponibili per le regole che seguono questo gruppo di regole nell'ACL Web. AWS WAF registra anche le etichette in base ai CloudWatch parametri di Amazon. Per informazioni generali sulle etichette e sui parametri delle etichette, consulta Etichette sulle richieste web e. Metriche e dimensioni delle etichette

> **Note**
>
> Questa tabella descrive l'ultima versione statica di questo gruppo di regole. Per le altre versioni, utilizzare il comando API DescribeManagedRuleGroup.

Nome regola	Descrizione ed etichetta
`JavaDeserializationRCE_HEADER`	Ispeziona le chiavi e i valori delle intestazioni delle richieste HTTP alla ricerca di modelli che indicano i tentativi di deserializzazione di Java Remote Command Execution (RCE), come le vulnerabilità RCE di Spring Core e Cloud Function (CVE-2022-22963, CVE-2022-22965). I modelli di esempio includono `(java.lang.Runtime).getRuntime().exec("whoami")` . **Warning** Questa regola controlla solo i primi 8 KB delle intestazioni di richiesta o le prime 200 intestazioni, a seconda del limite raggiunto per primo, e utilizza `Continue` l'opzione per la gestione di contenuti di grandi dimensioni. Per ulteriori informazioni, consulta Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF.

Nome regola	Descrizione ed etichetta
	Operazione delle regole: Block Etichetta: `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Header`

Nome regola	Descrizione ed etichetta
`JavaDeserializationRCE_BODY`	Ispeziona il corpo della richiesta alla ricerca di modelli che indicano i tentativi di deserializzazione di Java Remote Command Execution (RCE), come le vulnerabilità RCE di Spring Core e Cloud Function (CVE-2022-22963, CVE-2022-22965). I modelli di esempio includono `(java.lang.Runtime).getRuntime().exec("whoami")` . **Warning** Questa regola ispeziona il corpo della richiesta solo fino al limite di dimensione del corpo per l'ACL Web e il tipo di risorsa. Per Application Load Balancer and AWS AppSync, il limite è fissato a 8 KB. Per CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, il limite predefinito è 16 KB e puoi aumentare il limite fino a 64 KB nella configurazione ACL web. Questa regola utilizza l'`Continue`opzione per la gestione di contenuti di grandi dimensioni. Per ulteriori informazioni, consulta Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Body`

Nome regola	Descrizione ed etichetta
`JavaDeserializationRCE_URIPATH`	Controlla l'URI della richiesta alla ricerca di modelli che indicano i tentativi di deseriali zzazione di Java Remote Command Execution (RCE), come le vulnerabilità RCE di Spring Core e Cloud Function (CVE-2022 -22963, CVE-2022-22965). I modelli di esempio includono `(java.lang.Runtime ).getRuntime().exec("whoami")` . Operazione delle regole: Block Etichetta: `awswaf:managed:aws:known-bad-inputs:JavaDeserializatio nRCE_URIPath`
`JavaDeserializationRCE_QUER YSTRING`	Ispeziona la stringa di query della richiesta alla ricerca di modelli che indicano i tentativi di deserializzazione di Java Remote Command Execution (RCE), come le vulnerabilità RCE di Spring Core e Cloud Function (CVE-2022 -22963, CVE-2022-22965). I modelli di esempio includono `(java.lang.Runtime ).getRuntime().exec("whoami")` . Operazione delle regole: Block Etichetta: `awswaf:managed:aws:known-bad-inputs:JavaDeserializatio nRCE_QueryString`

Nome regola	Descrizione ed etichetta
`Host_localhost_HEADER`	Controlla l'intestazione host nella richiesta per i modelli che indicano localhost. I modelli di esempio includono `localhost` . Operazione delle regole: Block Etichetta: `awswaf:managed:aws:known-bad-inputs:Host_Localhost_Header`
`PROPFIND_METHOD`	Controlla il metodo HTTP nella richiesta per `PROPFIND`, che è un metodo simile a `HEAD`, ma con l'intenzione aggiuntiva di esfiltrare gli oggetti XML. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:known-bad-inputs:Propfind_Method`
`ExploitablePaths_URIPATH`	Controlla il percorso URI per i tentativi di accesso ai percorsi delle applicazioni Web sfruttabili. I modelli di esempio includono percorsi come `web-inf`. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:known-bad-inputs:ExploitablePaths_URIPath`

Nome regola	Descrizione ed etichetta
`Log4JRCE_HEADER`	Ispeziona le chiavi e i valori delle intestazioni di richiesta per verificare la presenza della vulnerabilità Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) e protegge dai tentativi di esecuzione di codice in modalità remota (RCE). I modelli di esempio includono `${jndi:ldap://example.com/}` . **Warning** Questa regola controlla solo i primi 8 KB delle intestazioni di richiesta o le prime 200 intestazioni, a seconda del limite raggiunto per primo, e utilizza `Continue` l'opzione per la gestione di contenuti di grandi dimensioni. Per ulteriori informazioni, consulta Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_Header`

Nome regola	Descrizione ed etichetta
`Log4JRCE_QUERYSTRING`	Ispeziona la stringa di query per verificare la presenza della vulnerabilità Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) e protegge dai tentativi di esecuzione di codice in modalità remota (RCE). I modelli di esempio includono `${jndi:ldap://example.com/}` . Operazione delle regole: Block Etichetta: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_QueryString`

Nome regola	Descrizione ed etichetta
`Log4JRCE_BODY`	Ispeziona il corpo per verificare la presenza della vulnerabilità Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) e protegge dai tentativi di esecuzione del codice remoto (RCE). I modelli di esempio includono `${jndi:ldap://example.com/}` . **Warning** Questa regola ispeziona il corpo della richiesta solo fino al limite di dimensione del corpo per l'ACL Web e il tipo di risorsa. Per Application Load Balancer and AWS AppSync, il limite è fissato a 8 KB. Per CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, il limite predefinito è 16 KB e puoi aumentare il limite fino a 64 KB nella configurazione ACL web. Questa regola utilizza l'`Continue`opzione per la gestione di contenuti di grandi dimensioni. Per ulteriori informazioni, consulta Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_Body`

Nome regola	Descrizione ed etichetta
`Log4JRCE_URIPATH`	Ispeziona il percorso URI per verificare la presenza della vulnerabilità Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) e protegge dai tentativi di esecuzione del codice remoto (RCE). I modelli di esempio includono `${jndi:ldap://example.com/}` . Operazione delle regole: Block Etichetta: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_URIPath`

Gruppi di regole specifici del caso d'uso

I gruppi di regole specifici per i casi d'uso forniscono una protezione incrementale per molti casi d'uso diversi. AWS WAF Scegli i gruppi di regole che si applicano alla tua applicazione.

> **Note**
>
> Le informazioni che pubblichiamo per le regole nei gruppi di regole AWS Managed Rules hanno lo scopo di fornirti informazioni sufficienti per utilizzare le regole, senza fornire informazioni che i malintenzionati potrebbero utilizzare per aggirarle. Se hai bisogno di più informazioni di quelle che trovi in questa documentazione, contatta il AWS Support Centro.

Gruppo di regole gestito dal database SQL

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

Il gruppo di regole Database SQL contiene regole per bloccare i modelli di richieste associati allo sfruttamento dei database SQL, ad esempio gli attacchi SQL injection. Ciò impedisce l'iniezione remota di query non autorizzate. Valuta l'uso di questo gruppo di regole se l'applicazione si interfaccia con un database SQL.

Questo gruppo di regole gestito aggiunge etichette alle richieste Web che valuta, che sono disponibili per le regole che seguono questo gruppo di regole nell'ACL Web. AWS WAF registra anche le

etichette in base ai CloudWatch parametri di Amazon. Per informazioni generali sulle etichette e sui parametri delle etichette, consulta Etichette sulle richieste web e. Metriche e dimensioni delle etichette

> **Note**
>
> Questa tabella descrive l'ultima versione statica di questo gruppo di regole. Per le altre versioni, utilizzare il comando API DescribeManagedRuleGroup.

Nome regola	Descrizione ed etichetta
`SQLi_QUERYARGUMENTS`	Utilizza la funzionalità integrata AWS WAF Istruzione regola attacco SQL Injection, con il livello di sensibilità impostato suLow, per ispezionare i valori di tutti i parametri di query alla ricerca di modelli che corrispondono al codice SQL dannoso. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:sql-database:SQLi_QueryArguments`
`SQLiExtendedPatterns_QUERYARGUMENTS`	Controlla i valori di tutti i parametri di query per individuare modelli che corrispondono a codice SQL dannoso. I modelli controllati da questa regola non sono coperti dalla regola`SQLi_QUERYARGUMENTS` . Operazione delle regole: Block Etichetta: `awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments`
`SQLi_BODY`	

Nome regola	Descrizione ed etichetta
	Utilizza la funzionalità integrata AWS WAF Istruzione regola attacco SQL Injection, con il livello di sensibilità impostato suLow, per ispezionare il corpo della richiesta alla ricerca di modelli che corrispondono al codice SQL dannoso. **Warning** Questa regola ispeziona il corpo della richiesta solo fino al limite di dimensione del corpo per l'ACL Web e il tipo di risorsa. Per Application Load Balancer and AWS AppSync, il limite è fissato a 8 KB. Per CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, il limite predefinito è 16 KB e puoi aumentare il limite fino a 64 KB nella configurazione ACL web. Questa regola utilizza l'`Continue`opzione per la gestione di contenuti di grandi dimensioni. Per ulteriori informazioni, consulta Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:sql-database:SQLi_Body`

Nome regola	Descrizione ed etichetta
`SQLiExtendedPatterns_BODY`	Ispeziona il corpo della richiesta alla ricerca di modelli che corrispondono al codice SQL dannoso. I modelli ricercati da questa regola non sono coperti dalla regola. `SQLi_BODY` **Warning** Questa regola ispeziona il corpo della richiesta solo fino al limite di dimensione del corpo per l'ACL Web e il tipo di risorsa. Per Application Load Balancer and AWS AppSync, il limite è fissato a 8 KB. Per CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, il limite predefinito è 16 KB e puoi aumentare il limite fino a 64 KB nella configurazione ACL web. Questa regola utilizza l'`Continue`opzione per la gestione di contenuti di grandi dimensioni. Per ulteriori informazioni, consulta Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:sql-database:SQLiExtendedPatterns_Body`

Nome regola	Descrizione ed etichetta
`SQLi_COOKIE`	Utilizza la funzionalità integrata AWS WAF Istruzione regola attacco SQL Injection, con il livello di sensibilità impostato suLow, per ispezionare le intestazioni dei cookie di richiesta alla ricerca di modelli che corrispon dono al codice SQL dannoso. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:sql-database:SQLi_Cookie`

Gruppo di regole gestito dal sistema operativo Linux

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

Il gruppo di regole del sistema operativo Linux contiene regole che bloccano i modelli di richieste associati allo sfruttamento di vulnerabilità specifiche di Linux, inclusi gli attacchi LFI (Local File Inclusion) specifici di Linux. Questo può aiutare a prevenire attacchi che espongono il contenuto dei file o eseguono codice a cui l'autore dell'attacco non avrebbe dovuto avere accesso. Valuta questo gruppo di regole se qualsiasi parte dell'applicazione viene eseguita su Linux. È consigliabile utilizzare questo gruppo di regole insieme al gruppo di regole Sistema operativo POSIX.

Questo gruppo di regole gestito aggiunge etichette alle richieste Web che valuta, che sono disponibili per le regole che seguono questo gruppo di regole nell'ACL Web. AWS WAF registra anche le etichette in base ai CloudWatch parametri di Amazon. Per informazioni generali sulle etichette e sui parametri delle etichette, consulta Etichette sulle richieste web e. Metriche e dimensioni delle etichette

> **Note**
>
> Questa tabella descrive l'ultima versione statica di questo gruppo di regole. Per le altre versioni, utilizzare il comando API DescribeManagedRuleGroup.

Nome regola	Descrizione ed etichetta
`LFI_URIPATH`	Controlla il percorso della richiesta per i tentativi di sfruttare le vulnerabilità LFI (Local File Inclusion) nelle applicazioni Web. I modelli di esempio includono file come `/proc/version` , che potrebbero fornire informazioni sul sistema operativo agli aggressori. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:linux-os:LFI_URIPath`
`LFI_QUERYSTRING`	Ispeziona i valori di querystring alla ricerca di tentativi di sfruttare le vulnerabilità di Local File Inclusion (LFI) nelle applicazioni Web. I modelli di esempio includono file come `/proc/version` , che potrebbero fornire informazioni sul sistema operativo agli aggressori. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:linux-os:LFI_QueryString`
`LFI_HEADER`	Esamina le intestazioni delle richieste per individuare eventuali tentativi di sfruttare le vulnerabilità LFI (Local File Inclusion) nelle applicazioni Web. I modelli di esempio includono file come `/proc/version` , che potrebbero fornire informazioni sul sistema operativo agli aggressori.

Nome regola	Descrizione ed etichetta
	Warning Questa regola ispeziona solo i primi 8 KB delle intestazioni di richiesta o le prime 200 intestazioni, a seconda del limite raggiunto per primo, e utilizza l'opzione per la gestione di contenuti di grandi dimensioni. `Continue` Per ulteriori informazioni, consulta Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:linux-os:LFI_Header`

gruppo di regole gestito dal sistema operativo POSIX

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

Il gruppo di regole del sistema operativo POSIX contiene regole che bloccano i modelli di richiesta associati allo sfruttamento di vulnerabilità specifiche di sistemi operativi POSIX e simili a POSIX, inclusi gli attacchi LFI (Local File Inclusion). Questo può aiutare a prevenire attacchi che espongono il contenuto dei file o eseguono codice a cui l'autore dell'attacco non avrebbe dovuto avere accesso. Valuta questo gruppo di regole se una parte dell'applicazione viene eseguita su un sistema operativo POSIX o simile a POSIX, inclusi Linux, AIX, HP-UX, macOS, Solaris, FreeBSD e OpenBSD.

Questo gruppo di regole gestito aggiunge etichette alle richieste Web che valuta, che sono disponibili per le regole che seguono questo gruppo di regole nell'ACL Web. AWS WAF registra anche le etichette in base ai CloudWatch parametri di Amazon. Per informazioni generali sulle etichette e sui parametri delle etichette, consulta Etichette sulle richieste web e. Metriche e dimensioni delle etichette

> **Note**
>
> Questa tabella descrive l'ultima versione statica di questo gruppo di regole. Per le altre versioni, utilizzare il comando API DescribeManagedRuleGroup.

Nome regola	Descrizione ed etichetta
`UNIXShellCommandsVariables_QUERYARGUMENTS`	Controlla i valori di tutti i parametri di query per i tentativi di sfruttare le vulnerabilità di command injection, LFI e path traversal nelle applicazioni Web eseguite su sistemi Unix. Gli esempi includono modelli come `echo $HOME` e `echo $PATH`. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QUERYARGUMENTS`
`UNIXShellCommandsVariables_BODY`	Controlla il corpo della richiesta per i tentativi di sfruttare le vulnerabilità di command injection, LFI e path traversal nelle applicazioni Web eseguite su sistemi Unix. Gli esempi includono modelli come `echo $HOME` e `echo $PATH`. **Warning** Questa regola controlla solo il corpo della richiesta fino al limite di dimensione del corpo per l'ACL Web e il tipo di risorsa. Per Application Load Balancer and AWS AppSync, il limite è fissato a 8 KB. Per CloudFront API Gateway,

Nome regola	Descrizione ed etichetta
	Amazon Cognito, App Runner e Verified Access, il limite predefinito è 16 KB e puoi aumentare il limite fino a 64 KB nella configurazione ACL web. Questa regola utilizza l'`Continue`opzione per la gestione di contenuti di grandi dimensioni. Per ulteriori informazioni, consulta Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_BODY`

Gruppo di regole gestito dal sistema operativo Windows

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

Il gruppo di regole del sistema operativo Windows contiene regole che bloccano i modelli di richiesta associati allo sfruttamento di vulnerabilità specifiche di Windows, come l'esecuzione remota di comandi. PowerShell Questo può aiutare a prevenire lo sfruttamento di vulnerabilità che consentono a un utente malintenzionato di eseguire comandi non autorizzati o eseguire codice dannoso. Valuta questo gruppo di regole se una parte dell'applicazione viene eseguita su un sistema operativo Windows.

Questo gruppo di regole gestito aggiunge etichette alle richieste Web che valuta, che sono disponibili per le regole che seguono questo gruppo di regole nell'ACL Web. AWS WAF registra anche le etichette in base ai CloudWatch parametri di Amazon. Per informazioni generali sulle etichette e sui parametri delle etichette, consulta Etichette sulle richieste web e. Metriche e dimensioni delle etichette

> **Note**
>
> Questa tabella descrive l'ultima versione statica di questo gruppo di regole. Per le altre versioni, utilizzare il comando API DescribeManagedRuleGroup.

Nome regola	Descrizione ed etichetta
`WindowsShellCommands_COOKIE`	Ispeziona le intestazioni dei cookie di richiesta per i tentativi di iniezione di WindowsShell comandi nelle applicazioni Web. I pattern di corrispondenza rappresentano WindowsShell i comandi. I modelli di esempio includono `|| nslookup e;cmd`. Operazione delle regole: Block Etichetta: `awswaf:managed:aws :windows-os:WindowsShellCom mands_Cookie`
`WindowsShellCommands_QUERYA RGUMENTS`	Controlla i valori di tutti i parametri di query per i tentativi di inserimento di WindowsShell comandi nelle applicazioni Web. I pattern di corrispondenza rappresentano WindowsShell i comandi. I modelli di esempio includono `|| nslookup e;cmd`. Operazione delle regole: Block Etichetta: `awswaf:managed:aws :windows-os:WindowsShellCom mands_QueryArguments`
`WindowsShellCommands_BODY`	Ispeziona il corpo della richiesta per i tentativi di iniezione di WindowsShell comandi nelle

Nome regola	Descrizione ed etichetta
	applicazioni Web. I pattern di corrispondenza rappresentano WindowsShell i comandi. I modelli di esempio includono `||nslookup` e `;cmd`. **Warning** Questa regola controlla solo il corpo della richiesta fino al limite di dimension e del corpo per l'ACL Web e il tipo di risorsa. Per Application Load Balancer and AWS AppSync, il limite è fissato a 8 KB. Per CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, il limite predefinito è 16 KB e puoi aumentare il limite fino a 64 KB nella configurazione ACL web. Questa regola utilizza l'`Continue`opzione per la gestione di contenuti di grandi dimensioni. Per ulteriori informazioni, consulta Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:windows-os:WindowsShellCommands_Body`

Nome regola	Descrizione ed etichetta
`PowerShellCommands_COOKIE`	Ispeziona le intestazioni dei cookie di richiesta per i tentativi di iniezione di PowerShell comandi nelle applicazioni Web. I pattern di corrispondenza rappresentano PowerShel l i comandi. Ad esempio, `Invoke-Ex pression` . Operazione delle regole: Block Etichetta: `awswaf:managed:aws :windows-os:PowerShellComma nds_Cookie`
`PowerShellCommands_QUERYARG UMENTS`	Controlla i valori di tutti i parametri di query per i tentativi di inserimento di PowerShell comandi nelle applicazioni Web. I pattern di corrispon denza rappresentano PowerShell i comandi. Ad esempio, `Invoke-Expression` . Operazione delle regole: Block Etichetta: `awswaf:managed:aws :windows-os:PowerShellComma nds_QueryArguments`

Nome regola	Descrizione ed etichetta
`PowerShellCommands_BODY`	Ispeziona il corpo della richiesta per i tentativi di iniezione di PowerShell comandi nelle applicazioni Web. I pattern di corrispondenza rappresentano PowerShell i comandi. Ad esempio, `Invoke-Expression` . **Warning** Questa regola controlla solo il corpo della richiesta fino al limite di dimensione del corpo per l'ACL Web e il tipo di risorsa. Per Application Load Balancer and AWS AppSync, il limite è fissato a 8 KB. Per CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, il limite predefinito è 16 KB e puoi aumentare il limite fino a 64 KB nella configurazione ACL web. Questa regola utilizza l'`Continue`opzione per la gestione di contenuti di grandi dimensioni. Per ulteriori informazioni, consulta Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:windows-os:PowerShellCommands_Body`

Gruppo di regole gestito dall'applicazione PHP

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

Il gruppo di regole applicazione PHP contiene regole che bloccano i modelli di richiesta associati allo sfruttamento di vulnerabilità specifiche per l'uso del linguaggio di programmazione PHP, inclusa l'iniezione di funzioni PHP non sicure. Questo può aiutare a prevenire lo sfruttamento di vulnerabilità che consentono a un utente malintenzionato di eseguire in remoto codici o comandi per i quali non è autorizzato. Valuta questo gruppo di regole se PHP è installato su qualsiasi server che si interfaccia con l'applicazione.

Questo gruppo di regole gestito aggiunge etichette alle richieste Web che valuta, che sono disponibili per le regole che seguono questo gruppo di regole nell'ACL Web. AWS WAF registra anche le etichette in base ai CloudWatch parametri di Amazon. Per informazioni generali sulle etichette e sui parametri delle etichette, consulta Etichette sulle richieste web e. Metriche e dimensioni delle etichette

> **Note**
>
> Questa tabella descrive l'ultima versione statica di questo gruppo di regole. Per le altre versioni, utilizzare il comando API DescribeManagedRuleGroup.

Nome regola	Descrizione ed etichetta
`PHPHighRiskMethodsVariables_HEADER`	Ispeziona tutte le intestazioni per i tentativi di iniezione di codice di script PHP. I modelli di esempio includono funzioni come `fsockopen` e la variabile superglobale `$_GET`. **Warning** Questa regola controlla solo i primi 8 KB delle intestazioni di richiesta o le prime 200 intestazioni, a seconda di quale limite viene raggiunto per primo, e utilizza l'opzione per la gestione di contenuti di grandi dimensioni.

Nome regola	Descrizione ed etichetta
	`Continue` Per ulteriori informazioni, consulta Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Header`
`PHPHighRiskMethodsVariables_QUERYSTRING`	Ispeziona tutto dopo il primo ? nell'URL della richiesta, alla ricerca di tentativi di inserimento del codice dello script PHP. I modelli di esempio includono funzioni come `fsockopen` e la variabile superglobale `$_GET`. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_QueryString`

Nome regola	Descrizione ed etichetta
`PHPHighRiskMethodsVariables_BODY`	Controlla i valori del corpo della richiesta per i tentativi di script code injection PHP. I modelli di esempio includono funzioni come `fsockopen` e la variabile superglobale `$_GET`. **Warning** Questa regola controlla solo il corpo della richiesta fino al limite di dimension e del corpo per l'ACL Web e il tipo di risorsa. Per Application Load Balancer and AWS AppSync, il limite è fissato a 8 KB. Per CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, il limite predefinito è 16 KB e puoi aumentare il limite fino a 64 KB nella configurazione ACL web. Questa regola utilizza l'`Continue`opzione per la gestione di contenuti di grandi dimensioni. Per ulteriori informazioni, consulta Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Body`

WordPress gruppo di regole gestito dall'applicazione

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

Il gruppo di regole WordPress dell'applicazione contiene regole che bloccano i modelli di richiesta associati allo sfruttamento di vulnerabilità specifiche dei siti. WordPress Dovresti valutare questo gruppo di regole se stai correndoWordPress. Questo gruppo di regole deve essere utilizzato insieme ai gruppi di regole Database SQL e Applicazione PHP.

Questo gruppo di regole gestito aggiunge etichette alle richieste Web che valuta, che sono disponibili per le regole che seguono questo gruppo di regole nell'ACL Web. AWS WAF registra anche le etichette in base ai CloudWatch parametri di Amazon. Per informazioni generali sulle etichette e sui parametri delle etichette, consulta Etichette sulle richieste web e. Metriche e dimensioni delle etichette

> **Note**
>
> Questa tabella descrive l'ultima versione statica di questo gruppo di regole. Per le altre versioni, utilizzare il comando API DescribeManagedRuleGroup.

Nome regola	Descrizione ed etichetta
`WordPressExploitableCommands_QUERYSTRING`	Controlla la stringa di query della richiesta alla ricerca di WordPress comandi ad alto rischio che possono essere sfruttati in installazioni o plugin vulnerabili. Gli esempi modelli includono comandi come `do-reset-wordpress` . Operazione delle regole: Block Etichetta: `awswaf:managed:aws:wordpress-app:WordPressExploitableCommands_QUERYSTRING`
`WordPressExploitablePaths_URIPATH`	Ispeziona il percorso URI della richiesta per WordPress file come`xmlrpc.php` , che sono noti per avere vulnerabilità facilmente sfruttabili.

Nome regola	Descrizione ed etichetta
	Operazione delle regole: Block Etichetta: `awswaf:managed:aws:wordpress-app:WordPressExploitablePaths_URIPATH`

Gruppi di regole Reputazione IP

I gruppi di regole di reputazione IP bloccano le richieste in base all'indirizzo IP di origine.

> **Note**
>
> Queste regole utilizzano l'indirizzo IP di origine della richiesta Web. Se il traffico passa attraverso uno o più proxy o sistemi di bilanciamento del carico, l'origine della richiesta Web conterrà l'indirizzo dell'ultimo proxy e non l'indirizzo di origine del client.

Scegli uno o più di questi gruppi di regole se desideri ridurre l'esposizione al traffico di bot, ai tentativi di sfruttamento o se stai imponendo restrizioni geografiche sui contenuti. Per la gestione dei bot, vedi anche. AWS WAF Gruppo di regole Bot Control

I gruppi di regole di questa categoria non forniscono notifiche di controllo delle versioni o di aggiornamento SNS.

> **Note**
>
> Le informazioni che pubblichiamo per le regole nei gruppi di regole AWS Managed Rules hanno lo scopo di fornirti informazioni sufficienti per utilizzare le regole, senza fornire informazioni che i malintenzionati potrebbero utilizzare per aggirarle. Se hai bisogno di più informazioni di quelle che trovi in questa documentazione, contatta il AWS Support Centro.

Gruppo di regole gestito con Amazon IP Reputation List

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

Il gruppo di regole dell'elenco di reputazione IP di Amazon contiene regole basate sull'intelligence di minacce interne Amazon. Ciò è utile se desideri bloccare gli indirizzi IP tipicamente associati a bot o ad altre minacce. Il blocco di questi indirizzi IP consente di mitigare i bot e ridurre il rischio che un utente malintenzionato scopra un'applicazione vulnerabile.

Questo gruppo di regole gestito aggiunge etichette alle richieste Web che valuta, che sono disponibili per le regole che seguono questo gruppo di regole nell'ACL Web. AWS WAF registra anche le etichette in base ai CloudWatch parametri di Amazon. Per informazioni generali sulle etichette e sui parametri delle etichette, consulta Etichette sulle richieste web e. Metriche e dimensioni delle etichette

Nome regola	Descrizione ed etichetta
`AWSManagedIPReputationList`	Esamina gli indirizzi IP che sono stati identificati come attivamente coinvolti in attività dannose. AWS WAF raccoglie l'elenco di indirizzi IP da varie fonti MadPot, tra cui uno strumento di intelligence sulle minacce che Amazon utilizza per proteggere i clienti dalla criminali tà informatica. Per ulteriori informazioni su MadPot, consulta. https://www.aboutamazon.com/news/aws/amazon-madpot-stops-cybersecurity-crime Operazione delle regole: Block Etichetta: `awswaf:managed:aws :amazon-ip-list:AWSManagedI PReputationList`
`AWSManagedReconnaissanceList`	Verifica la presenza di connessioni provenien ti da indirizzi IP che eseguono la ricognizione rispetto alle risorse. AWS Operazione delle regole: Block

Nome regola	Descrizione ed etichetta
	Etichetta: `awswaf:managed:aws:amazon-ip-list:AWSManagedReconnaissanceList`
`AWSManagedIPDDoSList`	Verifica la presenza di indirizzi IP che sono stati identificati come coinvolti attivamente in attività DDoS. Operazione delle regole: Count Etichetta: `awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList`

Gruppo di regole gestito con elenco IP anonimo

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

Il gruppo di regole dell'elenco di IP anonimi contiene regole per bloccare le richieste provenienti da servizi che consentono l'offuscamento dell'identità degli spettatori. Queste includono le richieste provenienti da VPN, proxy, nodi Tor e provider di web hosting. Questo gruppo di regole è utile se si desidera filtrare i visualizzatori che potrebbero tentare di nascondere la propria identità dall'applicazione. Bloccare gli indirizzi IP di questi servizi può aiutare a mitigare i bot e l'evasione delle restrizioni geografiche.

Questo gruppo di regole gestito aggiunge etichette alle richieste Web che valuta, che sono disponibili per le regole che seguono questo gruppo di regole nell'ACL web. AWS WAF registra anche le etichette in base ai CloudWatch parametri di Amazon. Per informazioni generali sulle etichette e sui parametri delle etichette, consulta Etichette sulle richieste web e. Metriche e dimensioni delle etichette

Nome regola	Descrizione ed etichetta
`AnonymousIPList`	Controlla un elenco di indirizzi IP di origini note per anonimizzare le informazioni del client,

Nome regola	Descrizione ed etichetta
	come nodi TOR, proxy temporanei e altri servizi di mascheramento. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:anonymous-ip-list:AnonymousIPList`
`HostingProviderIPList`	Cerca un elenco di indirizzi IP dei provider di web hosting e cloud, che hanno meno probabilità di generare traffico verso gli utenti finali. L'elenco IP non include AWS gli indirizzi IP. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:anonymous-ip-list:HostingProviderIPList`

AWS WAF Gruppo di regole per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control

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

Il gruppo AWS WAF di regole gestito per la prevenzione delle frodi (ACFP) per la creazione di account di Fraud Control etichetta e gestisce le richieste che potrebbero far parte di tentativi fraudolenti di creazione di account. Il gruppo di regole esegue questa operazione esaminando le richieste di creazione di account che i clienti inviano agli endpoint di registrazione e creazione dell'account dell'applicazione.

Il gruppo di regole ACFP esamina i tentativi di creazione degli account in vari modi, per darvi visibilità e controllo sulle interazioni potenzialmente dannose. Il gruppo di regole utilizza i token di richiesta per raccogliere informazioni sul browser del client e sul livello di interattività umana nella creazione della richiesta di creazione dell'account. Il gruppo di regole rileva e gestisce i tentativi di creazione di account in blocco aggregando le richieste per indirizzo IP e sessione client e aggregando, in base alle informazioni fornite sull'account, come l'indirizzo fisico e il numero di telefono. Inoltre, il gruppo di

regole rileva e blocca la creazione di nuovi account utilizzando credenziali compromesse, il che aiuta a proteggere il livello di sicurezza dell'applicazione e dei nuovi utenti.

Utilizzo di questo gruppo di regole

Questo gruppo di regole richiede una configurazione personalizzata, che include la specificazione dei percorsi di registrazione e creazione dell'account dell'applicazione. Salvo dove diversamente indicato, le regole di questo gruppo di regole esaminano tutte le richieste inviate dai client a questi due endpoint. Per configurare e implementare questo gruppo di regole, consulta la guida all'indirizzo. AWS WAF Fraud Control creazione di account e prevenzione delle frodi (ACFP)

> **Note**
>
> Quando utilizzi questo gruppo di regole gestito, ti vengono addebitati costi aggiuntivi. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

Questo gruppo di regole fa parte delle protezioni intelligenti di mitigazione delle minacce di. AWS WAF Per informazioni, consulta AWS WAF mitigazione intelligente delle minacce.

Per contenere i costi e avere la certezza di gestire il traffico web come desideri, utilizza questo gruppo di regole in conformità alle indicazioni riportate in. Le migliori pratiche per la mitigazione intelligente delle minacce

Questo gruppo di regole non è disponibile per l'uso con i pool di utenti di Amazon Cognito. Non puoi associare un ACL web che utilizza questo gruppo di regole a un pool di utenti e non puoi aggiungere questo gruppo di regole a un ACL web già associato a un pool di utenti.

Questo gruppo di regole non fornisce notifiche di controllo delle versioni o di aggiornamento SNS.

Etichette aggiunte da questo gruppo di regole

Questo gruppo di regole gestito aggiunge etichette alle richieste Web che valuta, che sono disponibili per le regole che seguono questo gruppo di regole nell'ACL Web. AWS WAF registra anche le etichette in base ai CloudWatch parametri di Amazon. Per informazioni generali sulle etichette e sui parametri delle etichette, consulta Etichette sulle richieste web e. Metriche e dimensioni delle etichette

Etichette con token

Questo gruppo di regole utilizza la gestione dei AWS WAF token per ispezionare ed etichettare le richieste Web in base allo stato dei relativi AWS WAF token. AWS WAF utilizza i token per il monitoraggio e la verifica delle sessioni dei clienti.

Per informazioni sui token e sulla gestione dei token, vedere. AWS WAF token di richiesta web

Per informazioni sui componenti dell'etichetta descritti qui, vedereRequisiti per la sintassi e la denominazione delle etichette.

Etichetta della sessione del client

L'etichetta `awswaf:managed:token:id:`*`identifier`* contiene un identificatore univoco utilizzato dalla gestione dei AWS WAF token per identificare la sessione client. L'identificatore può cambiare se il client acquisisce un nuovo token, ad esempio dopo aver scartato il token che stava utilizzando.

> **Note**
>
> AWS WAF non riporta le CloudWatch metriche di Amazon per questa etichetta.

Etichette di stato dei token: etichetta i prefissi dello spazio dei nomi

Le etichette di stato dei token riportano lo stato del token e le informazioni sulla sfida e sul CAPTCHA in esso contenute.

Ogni etichetta di stato del token inizia con uno dei seguenti prefissi dello spazio dei nomi:

- `awswaf:managed:token:`— Utilizzata per riportare lo stato generale del token e per riportare lo stato delle informazioni sulla sfida del token.
- `awswaf:managed:captcha:`— Utilizzato per riportare lo stato delle informazioni CAPTCHA del token.

Etichette di stato dei token: nomi delle etichette

Dopo il prefisso, il resto dell'etichetta fornisce informazioni dettagliate sullo stato del token:

- `accepted`— Il token di richiesta è presente e contiene quanto segue:
  - Una sfida o una soluzione CAPTCHA valida.

- Una sfida o un timestamp CAPTCHA non scaduti.
- Una specifica di dominio valida per l'ACL web.

Esempio: l'etichetta `awswaf:managed:token:accepted` indica che il token delle richieste Web ha una soluzione di sfida valida, un timestamp della sfida non scaduto e un dominio valido.

- `rejected`— Il token di richiesta è presente ma non soddisfa i criteri di accettazione.

  Oltre all'etichetta rifiutata, la gestione dei token aggiunge uno spazio dei nomi e un nome personalizzati per indicare il motivo.

  - `rejected:not_solved`— Al token manca la sfida o la soluzione CAPTCHA.
  - `rejected:expired`— La sfida o il timestamp CAPTCHA del token sono scaduti, in base ai tempi di immunità del token configurati dall'ACL web.
  - `rejected:domain_mismatch`— Il dominio del token non corrisponde alla configurazione del dominio token dell'ACL Web.
  - `rejected:invalid`— non è AWS WAF riuscito a leggere il token indicato.

  Esempio: `awswaf:managed:captcha:rejected` le etichette `awswaf:managed:captcha:rejected:expired` indicano che la richiesta è stata rifiutata perché il timestamp CAPTCHA nel token ha superato il tempo di immunità del token CAPTCHA configurato nell'ACL web.
- `absent`— La richiesta non ha il token o il gestore del token non è riuscito a leggerlo.

  Esempio: l'etichetta `awswaf:managed:captcha:absent` indica che la richiesta non ha il token.

Etichette ACFP

Questo gruppo di regole genera etichette con il prefisso dello spazio dei nomi `awswaf:managed:aws:acfp:` seguito dallo spazio dei nomi e dal nome dell'etichetta personalizzati. Il gruppo di regole potrebbe aggiungere più di un'etichetta a una richiesta.

È possibile recuperare tutte le etichette per un gruppo di regole tramite l'API `DescribeManagedRuleGroup` chiamando. Le etichette sono elencate nella `AvailableLabels` proprietà nella risposta.

Elenco delle regole di prevenzione delle frodi per la creazione di account

Questa sezione elenca le regole ACFP `AWSManagedRulesACFPRuleSet` e le etichette che le regole del gruppo di regole aggiungono alle richieste web.

> **Note**
>
> Le informazioni che pubblichiamo per le regole nei gruppi di regole AWS Managed Rules hanno lo scopo di fornirti informazioni sufficienti per utilizzare le regole, senza fornire informazioni che i malintenzionati potrebbero utilizzare per aggirare le regole. Se hai bisogno di più informazioni di quelle che trovi in questa documentazione, contatta il AWS Support Centro.

Tutte le regole di questo gruppo di regole richiedono un token di richiesta web, ad eccezione delle prime due `UnsupportedCognitoIDP` e`AllRequests`. Per una descrizione delle informazioni fornite dal token, vedereCaratteristiche del token.

Salvo dove diversamente indicato, le regole di questo gruppo di regole esaminano tutte le richieste che i client inviano ai percorsi delle pagine di registrazione e creazione dell'account forniti nella configurazione del gruppo di regole. Per informazioni sulla configurazione di questo gruppo di regole, vedere. AWS WAF Fraud Control creazione di account e prevenzione delle frodi (ACFP)

Nome regola	Descrizione ed etichetta
`UnsupportedCognitoIDP`	Esamina il traffico web diretto a un pool di utenti di Amazon Cognito. ACFP non è disponibile per l'uso con i pool di utenti di Amazon Cognito e questa regola aiuta a garantire che le altre regole del gruppo di regole ACFP non vengano utilizzate per valutare il traffico del pool di utenti. Operazione delle regole: Block Etichetta: `awswaf:managed:aws :acfp:unsupported:cognito_idp`
`AllRequests`	Applica l'azione della regola alle richieste che accedono al percorso della pagina di registraz ione. Il percorso della pagina di registrazione viene configurato quando si configura il gruppo di regole.

Nome regola	Descrizione ed etichetta
	Per impostazione predefinita, questa regola si applica Challenge alle richieste. Applicando questa azione, la regola assicura che il client acquisisca un token di sfida prima che qualsiasi richiesta venga valutata dal resto delle regole del gruppo di regole. Assicurati che gli utenti finali carichino il percorso della pagina di registrazione prima di inviare una richiesta di creazione dell'account. I token vengono aggiunti alle richieste dagli SDK di integrazione delle applicazioni client e dalle azioni CAPTCHA delle regole e. Challenge Per un'acquisizione di token più efficiente, consigliamo vivamente di utilizzar e gli SDK di integrazione delle applicazioni. Per ulteriori informazioni, consulta AWS WAF integrazione delle applicazioni client. Operazione delle regole: Challenge Etichetta: nessuna

Nome regola	Descrizione ed etichetta
`RiskScoreHigh`	Esamina le richieste di creazione di account con indirizzi IP o altri fattori considerati altamente sospetti. Questa valutazione si basa in genere su più fattori che contribuiscono, come è possibile vedere nelle `risk_score` etichette che il gruppo di regole aggiunge alla richiesta. Operazione delle regole: Block Etichetta: `awswaf:managed:aws :acfp:risk_score:high` È inoltre possibile applicare la regola `medium` o assegnare `low` dei punteggi di rischio alla richiesta. Se AWS WAF non riesce a valutare il punteggio di rischio per la richiesta web, la regola aggiunge l'etichetta `awswaf:ma naged:aws:acfp:risk_score:e valuation_failed` Inoltre, la regola aggiunge etichette con lo spazio dei nomi `awswaf:managed:aws :acfp:risk_score:contributo r:` che includono lo stato di valutazione del punteggio di rischio e i risultati relativi a specifici fattori che contribuiscono al punteggio di rischio, come le valutazioni della reputazione IP e delle credenziali rubate.

Nome regola	Descrizione ed etichetta
`SignalCredentialCompromised`	Cerca nel database delle credenziali rubate le credenziali inviate nella richiesta di creazione dell'account. Questa regola garantisce che i nuovi clienti inizializzino i propri account con un livello di sicurezza positivo. **Note** Puoi aggiungere una risposta di blocco personalizzata per descrivere il problema all'utente finale e dirgli come procedere. Per informazioni, consulta Esempio ACFP: risposta personalizzata per credenziali compromesse. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:acfp:signal:credential_compromised` Il gruppo di regole applica la seguente etichetta correlata, ma non interviene su di essa, poiché non tutte le richieste di creazione dell'account avranno credenziali: `awswaf:managed:aws:acfp:signal:missing_credential`

Nome regola	Descrizione ed etichetta
`SignalClientInteractivityAbsentLow`	Controlla il token della richiesta di creazione dell'account alla ricerca di dati che indichino un'interattività umana anomala con l'applicazione. L'interattività umana viene rilevata attraverso interazioni come i movimenti del mouse e la pressione dei tasti. Se la pagina ha un modulo HTML, l'interattività umana include le interazioni con il modulo. **Note** Questa regola esamina solo le richieste relative al percorso di creazione dell'account e viene valutata solo se hai implementato gli SDK di integrazione delle applicazioni. Le implementazioni SDK acquisiscono passivamente l'interattività umana e archiviano le informazioni nel token di richiesta. Per ulteriori informazioni, consultare Caratteristiche del token e AWS WAF integrazione delle applicazioni client. Operazione delle regole: CAPTCHA Etichetta: nessuna. La regola determina una corrispondenza in base a diversi fattori, quindi non esiste un'etichetta individuale valida per ogni possibile scenario di incontro. Il gruppo di regole può applicare una o più delle seguenti etichette alle richieste:

Nome regola	Descrizione ed etichetta

	`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`	Esamina la richiesta di indicatori che indicano che il browser del client potrebbe essere automatizzato. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:acfp:signal:automated_browser`
`SignalBrowserInconsistency`	Ispeziona il token della richiesta alla ricerca di dati di interrogazione del browser non coerenti. Per ulteriori informazioni, consulta Caratteristiche del token. Operazione delle regole: CAPTCHA Etichetta: `awswaf:managed:aws:acfp:signal:browser_inconsistency`

Nome regola	Descrizione ed etichetta
`VolumetricIpHigh`	Verifica la presenza di elevati volumi di richieste di creazione di account inviate da singoli indirizzi IP. Un volume elevato è costituito da più di 20 richieste in una finestra di 10 minuti. **Note** Le soglie applicate da questa regola possono variare leggermente a causa della latenza. Per un volume elevato, alcune richieste potrebbero superare il limite prima che venga applicata l'azione della regola. Operazione delle regole: CAPTCHA Etichetta: `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:high` La regola applica le seguenti etichette alle richieste con volumi medi (16-20 richieste per finestra di 10 minuti) e volumi bassi (11-15 richieste per finestra di 10 minuti), ma non interviene su di esse: `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:medium` e. `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:low`

Nome regola	Descrizione ed etichetta
`VolumetricSessionHigh`	Verifica la presenza di volumi elevati di richieste di creazione di account inviate da singole sessioni client. Un volume elevato è costituito da più di 10 richieste in una finestra di 30 minuti. **Note** Le soglie applicate da questa regola possono variare leggermente a causa della latenza. Alcune richieste potrebbero superare il limite prima che venga applicata l'azione della regola. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:high` Il gruppo di regole applica le seguenti etichette alle richieste con volumi medi (6-10 richieste per finestra di 30 minuti) e volumi bassi (2-5 richieste per finestra di 30 minuti), ma non interviene su di esse: `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:medium` e. `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:low`

Nome regola	Descrizione ed etichetta
`AttributeUsernameTraversalHigh`	Verifica la presenza di un tasso elevato di richieste di creazione di account da una singola sessione client che utilizza nomi utente diversi. La soglia per una valutazione elevata è superiore a 10 richieste in 30 minuti. **Note** Le soglie applicate da questa regola possono variare leggermente a causa della latenza. Alcune richieste potrebbero superare il limite prima che venga applicata l'azione della regola. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:high` Il gruppo di regole applica le seguenti etichette alle richieste con volumi medi (6-10 richieste per finestra di 30 minuti) e volumi bassi (2-5 richieste per finestra di 30 minuti) di richieste di attraversamento del nome utente, ma non interviene su di esse: e. `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:medium` `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:low`

Nome regola	Descrizione ed etichetta
`VolumetricPhoneNumberHigh`	Verifica la presenza di volumi elevati di richieste di creazione di account che utilizzano lo stesso numero di telefono. La soglia per una valutazione elevata è superiore a 10 richieste in 30 minuti. **Note** Le soglie applicate da questa regola possono variare leggermente a causa della latenza. Alcune richieste potrebbero superare il limite prima che venga applicata l'azione della regola. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:high` Il gruppo di regole applica le seguenti etichette alle richieste con volumi medi (6-10 richieste per finestra di 30 minuti) e volumi bassi (2-5 richieste per finestra di 30 minuti), ma non interviene su di esse: `awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:medium` e. `awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:low`

Nome regola	Descrizione ed etichetta
`VolumetricAddressHigh`	Verifica la presenza di volumi elevati di richieste di creazione di account che utilizzan o lo stesso indirizzo fisico. La soglia per una valutazione elevata è superiore a 100 richieste per finestra di 30 minuti. **Note** Le soglie applicate da questa regola possono variare leggermente a causa della latenza. Alcune richieste potrebbero superare il limite prima che venga applicata l'azione della regola. Operazione delle regole: Block Etichetta: `awswaf:managed:aws :acfp:aggregate:volumetric: address:high`

Nome regola	Descrizione ed etichetta
`VolumetricAddressLow`	Verifica la presenza di volumi bassi e medi di richieste di creazione di account che utilizzano lo stesso indirizzo fisico. La soglia per una valutazione media è superiore a 51-100 richieste per finestra di 30 minuti, mentre per una valutazione bassa è di 11-50 richieste per finestra di 30 minuti. La regola applica l'azione per volumi medi o bassi. **Note** Le soglie applicate da questa regola possono variare leggermente a causa della latenza. Alcune richieste potrebbero superare il limite prima che venga applicata l'azione della regola. Operazione delle regole: CAPTCHA Etichetta: `awswaf:managed:aws:acfp:aggregate:volumetric:address:low` o `awswaf:managed:aws:acfp:aggregate:volumetric:address:medium`

Nome regola	Descrizione ed etichetta
`VolumetricIPSuccessfulResponse`	Verifica la presenza di un volume elevato di richieste di creazione di account andate a buon fine per un singolo indirizzo IP. Questa regola aggrega le risposte di successo provenienti dalla risorsa protetta alle richieste di creazione di account. La soglia per una valutazione elevata è superiore a 10 richieste per finestra di 10 minuti. Questa regola aiuta a proteggersi dai tentativi di creazione di account in blocco. Ha una soglia inferiore rispetto alla regola`VolumetricIpHigh` , che conta solo le richieste. Se hai configurato il gruppo di regole per ispezionare il corpo della risposta o i componenti JSON, AWS WAF puoi ispezionare i primi 65.536 byte (64 KB) di questi tipi di componenti per individuare gli indicatori di successo o di fallimento. Questa regola applica l'azione e l'etichettatura della regola alle nuove richieste Web provenienti da un indirizzo IP, in base alle risposte di successo e di fallimento della risorsa protetta ai recenti tentativi di accesso dallo stesso indirizzo IP. Quando configuri il gruppo di regole, definisci come contare i successi e gli insuccessi.

Nome regola	Descrizione ed etichetta
	Note AWS WAF valuta questa regola solo negli ACL Web che proteggono le distribuzioni Amazon CloudFront .
	Note Le soglie applicate da questa regola possono variare leggermente a causa della latenza. È possibile che il client invii più tentativi di creazione di account riusciti rispetto a quelli consentiti prima che la regola inizi a corrispondere nei tentativi successivi.
	Operazione delle regole: Block Etichetta: `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:high` Il gruppo di regole applica anche le seguenti etichette correlate alle richieste, senza alcuna azione associata. Tutti i conteggi si riferiscono a una finestra di 10 minuti. `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:medium` per più di 5 richieste riuscite, `awswaf:managed:aws:acfp:aggregate:volumetric:`

Nome regola	Descrizione ed etichetta
	`ip:successful_creation_response:low` per più di 1 richiesta riuscita, `awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:high` per più di 10 richieste non riuscite, `awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:medium` per più di 5 richieste non riuscite e `awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:low` per più di 1 richiesta non riuscita.

Nome regola	Descrizione ed etichetta
`VolumetricSessionSuccessful Response`	Verifica la presenza di un basso volume di risposte riuscite provenienti dalla risorsa protetta alle richieste di creazione di account inviate da una singola sessione client. Questo aiuta a proteggersi dai tentativi di creazione di account in blocco. La soglia per una valutazio ne bassa è superiore a 1 richiesta per finestra di 30 minuti. Questo aiuta a proteggersi dai tentativi di creazione di account in blocco. Questa regola utilizza una soglia inferiore rispetto alla regola`VolumetricSessionHigh` , che tiene traccia solo delle richieste. Se hai configurato il gruppo di regole per ispezionare il corpo della risposta o i componenti JSON, AWS WAF puoi ispeziona re i primi 65.536 byte (64 KB) di questi tipi di componenti per individuare gli indicatori di successo o di fallimento. Questa regola applica l'azione e l'etichettatura della regola alle nuove richieste web provenien ti da una sessione client, in base alle risposte di successo e di fallimento della risorsa protetta ai recenti tentativi di accesso della stessa sessione client. Quando configuri il gruppo di regole, definisci come contare i successi e gli insuccessi.

Nome regola	Descrizione ed etichetta
	Note AWS WAF valuta questa regola solo negli ACL Web che proteggono le distribuzioni Amazon CloudFront .
	Note Le soglie applicate da questa regola possono variare leggermente a causa della latenza. È possibile che il client invii più tentativi falliti di creazione di account rispetto a quelli consentit i prima che la regola inizi a corrispon dere nei tentativi successivi.
	Operazione delle regole: Block Etichetta: `awswaf:managed:aws :acfp:aggregate:volumetric: session:successful_creation _response:low` Il gruppo di regole applica anche le seguenti etichette correlate alle richieste. Tutti i conteggi si riferiscono a una finestra di 30 minuti. `awswaf:managed:aws:acfp:agg regate:volumetric:session:s uccessful_creation_response :high` per più di 10 richieste riuscite, `awswaf:managed:aws:acfp:agg regate:volumetric:session:s`

Nome regola	Descrizione ed etichetta
	`uccessful_creation_response :medium` per più di 5 richieste riuscite, `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:high` per più di 10 richieste non riuscite, `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:medium` per più di 5 richieste non riuscite e `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:low` per più di 1 richiesta non riuscita.
`VolumetricSessionTokenReuseIp`	Esamina le richieste di creazione di account per l'uso di un singolo token tra più di 5 indirizzi IP distinti. **Note** Le soglie applicate da questa regola possono variare leggermente a causa della latenza. Alcune richieste potrebbero superare il limite prima che venga applicata l'azione della regola. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:token_reuse:ip`

AWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi

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

Il gruppo di regole gestito da AWS WAF Fraud Control Account Takeover Prevention (ATP) etichetta e gestisce le richieste che potrebbero far parte di tentativi malevoli di acquisizione di account. Il gruppo di regole esegue questa operazione esaminando i tentativi di accesso che i client inviano all'endpoint di accesso dell'applicazione.

- Richiedi un'ispezione: l'ATP ti offre visibilità e controllo sui tentativi di accesso anomali e sui tentativi di accesso che utilizzano credenziali rubate, per prevenire acquisizioni di account che potrebbero portare ad attività fraudolente. L'ATP verifica le combinazioni di e-mail e password confrontandole con il proprio database di credenziali rubate, che viene aggiornato regolarmente man mano che nuove credenziali trapelate vengono trovate sul dark web. L'ATP aggrega i dati in base all'indirizzo IP e alla sessione del client, per rilevare e bloccare i client che inviano troppe richieste di natura sospetta.
- Ispezione delle risposte: per CloudFront le distribuzioni, oltre a controllare le richieste di accesso in entrata, il gruppo di regole ATP controlla le risposte dell'applicazione ai tentativi di accesso, per tenere traccia delle percentuali di successo e di fallimento. Utilizzando queste informazioni, ATP può bloccare temporaneamente le sessioni client o gli indirizzi IP con troppi errori di accesso. AWS WAF esegue l'ispezione della risposta in modo asincrono, in modo da non aumentare la latenza del traffico web.

Utilizzo di questo gruppo di regole

Questo gruppo di regole richiede una configurazione specifica. Per configurare e implementare questo gruppo di regole, consulta la guida all'indirizzoAWS WAF Controllo delle frodi e prevenzione delle acquisizioni di conti (ATP).

Questo gruppo di regole fa parte delle protezioni intelligenti per la mitigazione delle minacce di. AWS WAF Per informazioni, consulta AWS WAF mitigazione intelligente delle minacce.

> **Note**
>
> Quando utilizzi questo gruppo di regole gestito, ti vengono addebitati costi aggiuntivi. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

Per contenere i costi e avere la certezza di gestire il traffico web come preferisci, utilizza questo gruppo di regole in conformità con le indicazioni riportate inLe migliori pratiche per la mitigazione intelligente delle minacce.

Questo gruppo di regole non è disponibile per l'uso con i pool di utenti di Amazon Cognito. Non puoi associare un ACL web che utilizza questo gruppo di regole a un pool di utenti e non puoi aggiungere questo gruppo di regole a un ACL web già associato a un pool di utenti.

Questo gruppo di regole non fornisce notifiche di controllo delle versioni o di aggiornamento SNS.

Etichette aggiunte da questo gruppo di regole

Questo gruppo di regole gestito aggiunge etichette alle richieste Web che valuta, che sono disponibili per le regole che seguono questo gruppo di regole nell'ACL Web. AWS WAF registra anche le etichette in base ai CloudWatch parametri di Amazon. Per informazioni generali sulle etichette e sui parametri delle etichette, consulta Etichette sulle richieste web e. Metriche e dimensioni delle etichette

Etichette con token

Questo gruppo di regole utilizza la gestione dei AWS WAF token per ispezionare ed etichettare le richieste Web in base allo stato dei relativi AWS WAF token. AWS WAF utilizza i token per il monitoraggio e la verifica delle sessioni dei clienti.

Per informazioni sui token e sulla gestione dei token, vedere. AWS WAF token di richiesta web

Per informazioni sui componenti dell'etichetta descritti qui, vedereRequisiti per la sintassi e la denominazione delle etichette.

Etichetta della sessione del client

L'etichetta `awswaf:managed:token:id:`*`identifier`* contiene un identificatore univoco utilizzato dalla gestione dei AWS WAF token per identificare la sessione client. L'identificatore può cambiare se il client acquisisce un nuovo token, ad esempio dopo aver scartato il token che stava utilizzando.

> **Note**
>
> AWS WAF non riporta i CloudWatch parametri Amazon per questa etichetta.

Etichette di stato dei token: etichetta i prefissi dello spazio dei nomi

Le etichette di stato dei token riportano lo stato del token e le informazioni sulla sfida e sul CAPTCHA in esso contenute.

Ogni etichetta di stato del token inizia con uno dei seguenti prefissi dello spazio dei nomi:

- `awswaf:managed:token:`— Utilizzata per riportare lo stato generale del token e per riportare lo stato delle informazioni sulla sfida del token.
- `awswaf:managed:captcha:`— Utilizzato per riportare lo stato delle informazioni CAPTCHA del token.

Etichette di stato dei token: nomi delle etichette

Dopo il prefisso, il resto dell'etichetta fornisce informazioni dettagliate sullo stato del token:

- `accepted`— Il token di richiesta è presente e contiene quanto segue:
  - Una sfida o una soluzione CAPTCHA valida.
  - Una sfida o un timestamp CAPTCHA non scaduti.
  - Una specifica di dominio valida per l'ACL web.

  Esempio: l'etichetta `awswaf:managed:token:accepted` indica che il token delle richieste Web ha una soluzione di sfida valida, un timestamp della sfida non scaduto e un dominio valido.
- `rejected`— Il token di richiesta è presente ma non soddisfa i criteri di accettazione.

  Oltre all'etichetta rifiutata, la gestione dei token aggiunge uno spazio dei nomi e un nome personalizzati per indicare il motivo.
  - `rejected:not_solved`— Al token manca la sfida o la soluzione CAPTCHA.
  - `rejected:expired`— La sfida o il timestamp CAPTCHA del token sono scaduti, in base ai tempi di immunità del token configurati dall'ACL web.
  - `rejected:domain_mismatch`— Il dominio del token non corrisponde alla configurazione del dominio token dell'ACL Web.
  - `rejected:invalid`— non è AWS WAF riuscito a leggere il token indicato.

  Esempio: `awswaf:managed:captcha:rejected` le etichette `awswaf:managed:captcha:rejected:expired` indicano che la richiesta è stata rifiutata perché il timestamp CAPTCHA nel token ha superato il tempo di immunità del token CAPTCHA configurato nell'ACL web.
- `absent`— La richiesta non ha il token o il gestore del token non è riuscito a leggerlo.

Esempio: l'etichetta `awswaf:managed:captcha:absent` indica che la richiesta non ha il token.

Etichette ATP

Il gruppo di regole gestito da ATP genera etichette con il prefisso dello spazio dei nomi `awswaf:managed:aws:atp:` seguito dallo spazio dei nomi e dal nome dell'etichetta personalizzati.

Il gruppo di regole può aggiungere una delle seguenti etichette oltre alle etichette indicate nell'elenco delle regole:

- `awswaf:managed:aws:atp:signal:credential_compromised`— Indica che le credenziali inviate nella richiesta si trovano nel database delle credenziali rubate.
- `awswaf:managed:aws:atp:aggregate:attribute:suspicious_tls_fingerprint`— Disponibile solo per le CloudFront distribuzioni protette di Amazon. Indica che una sessione client ha inviato più richieste che utilizzavano un'impronta digitale TLS sospetta.
- `awswaf:managed:aws:atp:aggregate:volumetric:session:token_reuse:ip`— Indica l'uso di un singolo token tra più di 5 indirizzi IP distinti. Le soglie applicate da questa regola possono variare leggermente a causa della latenza. Alcune richieste potrebbero superare il limite prima che l'etichetta venga applicata.

È possibile recuperare tutte le etichette per un gruppo di regole tramite l'API `DescribeManagedRuleGroup` chiamando. Le etichette sono elencate nella `AvailableLabels` proprietà nella risposta.

Elenco delle regole di prevenzione dell'acquisizione di account

Questa sezione elenca le regole ATP `AWSManagedRulesATPRuleSet` e le etichette che le regole del gruppo di regole aggiungono alle richieste web.

> **Note**
>
> Le informazioni che pubblichiamo per le regole nei gruppi di regole AWS Managed Rules hanno lo scopo di fornirti informazioni sufficienti per utilizzare le regole, senza fornire informazioni che i malintenzionati potrebbero utilizzare per aggirarle. Se hai bisogno di più informazioni di quelle che trovi in questa documentazione, contatta il AWS Support Centro.

Nome regola	Descrizione ed etichetta
`UnsupportedCognitoIDP`	Esamina il traffico web diretto a un pool di utenti di Amazon Cognito. L'ATP non è disponibile per l'uso con i pool di utenti di Amazon Cognito e questa regola aiuta a garantire che le altre regole del gruppo di regole ATP non vengano utilizzate per valutare il traffico del pool di utenti. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:atp:unsupported:cognito_idp`
`VolumetricIpHigh`	Verifica la presenza di elevati volumi di richieste inviate da singoli indirizzi IP. Un volume elevato è costituito da più di 20 richieste in una finestra di 10 minuti. **Note** Le soglie applicate da questa regola possono variare leggermente a causa della latenza. Per un volume elevato, alcune richieste potrebbero superare il limite prima che venga applicata l'azione della regola. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:atp:aggregate:volumetric:ip:high`

Nome regola	Descrizione ed etichetta
	Il gruppo di regole applica le seguenti etichette alle richieste con volumi medi (16-20 richieste per finestra di 10 minuti) e volumi bassi (11-15 richieste per finestra di 10 minuti), ma non interviene su di esse: `awswaf:managed:aws:atp:aggregate:volumetric:ip:medium` e. `awswaf:managed:aws:atp:aggregate:volumetric:ip:low`

Nome regola	Descrizione ed etichetta
`VolumetricSession`	Verifica la presenza di volumi elevati di richieste inviate da singole sessioni client. La soglia è superiore a 20 richieste per finestra di 30 minuti. Questa ispezione si applica solo quando la richiesta web ha un token. I token vengono aggiunti alle richieste dagli SDK di integrazione delle applicazioni e dalle azioni CAPTCHA delle regole e. Challenge Per ulteriori informazioni, consulta AWS WAF token di richiesta web. **Note** Le soglie applicate da questa regola possono variare leggermente a causa della latenza. Alcune richieste potrebbero superare il limite prima che venga applicata l'azione della regola. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:atp:aggregate:volumetric:session`

Nome regola	Descrizione ed etichetta
`AttributeCompromisedCredentials`	Verifica la presenza di più richieste provenien ti dalla stessa sessione client che utilizzano credenziali rubate. Operazione delle regole: Block Etichetta: `awswaf:managed:aws :atp:aggregate:attribute:co mpromised_credentials`
`AttributeUsernameTraversal`	Verifica la presenza di più richieste dalla stessa sessione client che utilizzano l'attraversamento del nome utente. Operazione delle regole: Block Etichetta: `awswaf:managed:aws :atp:aggregate:attribute:us ername_traversal`
`AttributePasswordTraversal`	Verifica la presenza di più richieste provenien ti dalla stessa sessione client che utilizzano l'incrocio delle password. Operazione delle regole: Block Etichetta: `awswaf:managed:aws :atp:aggregate:attribute:pa ssword_traversal`

Nome regola	Descrizione ed etichetta
`AttributeLongSession`	Verifica la presenza di più richieste provenien ti dalla stessa sessione client che utilizzano sessioni di lunga durata. Questa ispezione si applica solo quando la richiesta web ha un token. I token vengono aggiunti alle richieste dagli SDK di integrazione delle applicazioni e dalle azioni CAPTCHA delle regole e. Challenge Per ulteriori informazioni, consulta AWS WAF token di richiesta web. Operazione delle regole: Block Etichetta: `awswaf:managed:aws :atp:aggregate:attribute:lo ng_session`
`TokenRejected`	Controlla le richieste con token che vengono rifiutate dalla gestione dei AWS WAF token. Questa ispezione si applica solo quando la richiesta web ha un token. I token vengono aggiunti alle richieste dagli SDK di integrazione delle applicazioni e dalle azioni CAPTCHA delle regole e. Challenge Per ulteriori informazioni, consulta AWS WAF token di richiesta web. Operazione delle regole: Block Etichetta: nessuna. Per verificare se il token è stato rifiutato, utilizza una regola di corrispon denza delle etichette da applicare sull'etichetta: `awswaf:managed:token:rejected`

Nome regola	Descrizione ed etichetta
`SignalMissingCredential`	Verifica la presenza di richieste con credenziali prive del nome utente o della password. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:atp:signal:missing_credential`

Nome regola	Descrizione ed etichetta
`VolumetricIpFailedLoginResponseHigh`	Verifica la presenza di indirizzi IP che recentemente sono stati all'origine di un tasso troppo elevato di tentativi di accesso non riusciti. Un volume elevato è costituito da più di 10 richieste di accesso non riuscite da un indirizzo IP in una finestra di 10 minuti. Se hai configurato il gruppo di regole per ispezionare il corpo della risposta o i componenti JSON, AWS WAF puoi ispeziona re i primi 65.536 byte (64 KB) di questi tipi di componenti per individuare gli indicatori di successo o di fallimento. Questa regola applica l'azione e l'etichettatura della regola alle nuove richieste Web provenien ti da un indirizzo IP, in base alle risposte di successo e di fallimento della risorsa protetta ai recenti tentativi di accesso dallo stesso indirizzo IP. Quando configuri il gruppo di regole, definisci come contare i successi e gli insuccessi. **Note** AWS WAF valuta questa regola solo negli ACL Web che proteggono le distribuzioni Amazon CloudFront. **Note** Le soglie applicate da questa regola possono variare leggermente a causa

Nome regola	Descrizione ed etichetta
	della latenza. È possibile che il client invii un numero di tentativi di accesso non riuscito superiore a quello consentit o prima che la regola inizi a corrispon dere nei tentativi successivi. Operazione delle regole: Block Etichetta: `awswaf:managed:aws :atp:aggregate:volumetric:i p:failed_login_response:high` Il gruppo di regole applica anche le seguenti etichette correlate alle richieste, senza alcuna azione associata. Tutti i conteggi si riferisco no a una finestra di 10 minuti. `awswaf:ma naged:aws:atp:aggregate:vol umetric:ip:failed_login_res ponse:medium` per più di 5 richieste non riuscite, `awswaf:managed:aws :atp:aggregate:volumetric:i p:failed_login_response:low` per più di 1 richiesta non riuscita, `awswaf:ma naged:aws:atp:aggregate:vol umetric:ip:successful_login _response:high` per più di 10 richieste riuscite, `awswaf:managed:aws:atp:aggr egate:volumetric:ip:success ful_login_response:medium` per più di 5 richieste riuscite e `awswaf:managed:aws :atp:aggregate:volumetric:i p:successful_login_response:low` per più di 1 richiesta riuscita.

Nome regola	Descrizione ed etichetta
`VolumetricSessionFailedLogi nResponseHigh`	Esamina le sessioni client che di recente sono state all'origine di una frequenza troppo elevata di tentativi di accesso falliti. Un volume elevato è costituito da più di 10 richieste di accesso non riuscite da una sessione client in una finestra di 30 minuti. Se hai configurato il gruppo di regole per ispezionare il corpo della risposta o i componenti JSON, AWS WAF puoi ispeziona re i primi 65.536 byte (64 KB) di questi tipi di componenti per individuare gli indicatori di successo o di fallimento. Questa regola applica l'azione e l'etichettatura della regola alle nuove richieste web provenien ti da una sessione client, in base alle risposte di successo e di fallimento della risorsa protetta ai recenti tentativi di accesso della stessa sessione client. Quando configuri il gruppo di regole, definisci come contare i successi e gli insuccessi. **Note** AWS WAF valuta questa regola solo negli ACL Web che proteggono le distribuzioni Amazon CloudFront . **Note** Le soglie applicate da questa regola possono variare leggermente a causa

Nome regola	Descrizione ed etichetta
	della latenza. È possibile che il client invii un numero di tentativi di accesso non riuscito superiore a quello consentit o prima che la regola inizi a corrispon dere nei tentativi successivi. Questa ispezione si applica solo quando la richiesta web ha un token. I token vengono aggiunti alle richieste dagli SDK di integrazione delle applicazioni e dalle azioni CAPTCHA delle regole e. Challenge Per ulteriori informazioni, consulta AWS WAF token di richiesta web. Operazione delle regole: Block Etichetta: `awswaf:managed:aws :atp:aggregate:volumetric:s ession:failed_login_respons e:high` Il gruppo di regole applica anche le seguenti etichette correlate alle richieste, senza alcuna azione associata. Tutti i conteggi si riferisco no a una finestra di 30 minuti. `awswaf:ma naged:aws:atp:aggregate:vol umetric:session:failed_logi n_response:medium` per più di 5 richieste non riuscite, `awswaf:managed:aws :atp:aggregate:volumetric:s ession:failed_login_respons e:low` per più di 1 richiesta non riuscita, `awswaf:managed:aws:atp:aggr egate:volumetric:session:su ccessful_login_response:high`

Nome regola	Descrizione ed etichetta
	per più di 10 richieste riuscite, `awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:medium` per più di 5 richieste riuscite e `awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:low` per più di 1 richiesta riuscita.

AWS WAF Gruppo di regole Bot Control

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

Il gruppo di regole gestito da Bot Control fornisce regole che gestiscono le richieste provenienti dai bot. I bot possono consumare risorse in eccesso, alterare le metriche aziendali, causare tempi di inattività ed eseguire attività dannose.

Livelli di protezione

Il gruppo di regole gestito da Bot Control offre due livelli di protezione tra cui puoi scegliere:

- Comune: rileva una varietà di bot che si identificano automaticamente, come framework di web scraping, motori di ricerca e browser automatici. Le protezioni Bot Control a questo livello identificano i bot più comuni utilizzando tecniche di rilevamento dei bot tradizionali, come l'analisi statica dei dati delle richieste. Le regole etichettano il traffico proveniente da questi bot e bloccano quello che non possono verificare.
- Mirato: include le protezioni di livello comune e aggiunge il rilevamento mirato per bot sofisticati che non si identificano automaticamente. Le protezioni mirate mitigano l'attività dei bot utilizzando una combinazione di limitazioni della velocità e sfide legate al CAPTCHA e al browser in background.
  - **`TGT_`**— Le regole che forniscono una protezione mirata hanno nomi che iniziano con. `TGT_` Tutte le protezioni mirate utilizzano tecniche di rilevamento come l'interrogazione del browser, l'impronta digitale e l'euristica comportamentale per identificare il traffico di bot non valido.
  - **`TGT_ML_`**— Le regole di protezione mirate che utilizzano l'apprendimento automatico hanno nomi che iniziano con. `TGT_ML_` Queste regole utilizzano l'analisi automatizzata e basata sull'apprendimento automatico delle statistiche sul traffico dei siti Web per rilevare comportamenti anomali indicativi di un'attività distribuita e coordinata dei bot. AWS WAF analizza

le statistiche sul traffico del sito Web, ad esempio timestamp, caratteristiche del browser e URL visitato in precedenza, per migliorare il modello di apprendimento automatico di Bot Control. Le funzionalità di machine learning sono abilitate per impostazione predefinita, ma puoi disabilitarle nella configurazione del gruppo di regole. Quando l'apprendimento automatico è disabilitato, AWS WAF non valuta queste regole.

Il livello di protezione mirato e l'istruzione della regola AWS WAF basata sulla frequenza forniscono entrambi una limitazione della velocità. Per un confronto tra le due opzioni, vedere. Opzioni per la limitazione della velocità nelle regole basate sulla velocità e nelle regole mirate di Bot Control

Utilizzo di questo gruppo di regole

Questo gruppo di regole fa parte delle protezioni intelligenti di mitigazione delle minacce di. AWS WAF Per informazioni, consulta AWS WAF mitigazione intelligente delle minacce.

> **Note**
>
> Quando utilizzi questo gruppo di regole gestito, ti vengono addebitati costi aggiuntivi. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

Per contenere i costi e avere la certezza di gestire il traffico web come preferisci, utilizza questo gruppo di regole in conformità alle indicazioni riportate inLe migliori pratiche per la mitigazione intelligente delle minacce.

Aggiorniamo periodicamente i nostri modelli di machine learning (ML) per adattarli alle regole basate su ML a livello di protezione mirato, per migliorare le previsioni dei bot. Le regole basate su ML hanno nomi che iniziano con. `TGT_ML_` Se notate un cambiamento improvviso e sostanziale nelle previsioni relative ai bot formulate da queste regole, contattateci tramite il vostro account manager o aprite un caso presso AWS Support Center.

Il gruppo di regole Bot Control non fornisce notifiche di aggiornamento SNS.

Etichette aggiunte da questo gruppo di regole

Questo gruppo di regole gestito aggiunge etichette alle richieste Web che valuta, che sono disponibili per le regole che seguono questo gruppo di regole nell'ACL Web. AWS WAF registra anche le etichette in base ai CloudWatch parametri di Amazon. Per informazioni generali sulle etichette e sui parametri delle etichette, consulta Etichette sulle richieste web e. Metriche e dimensioni delle etichette

Etichette con token

Questo gruppo di regole utilizza la gestione dei AWS WAF token per ispezionare ed etichettare le richieste Web in base allo stato dei relativi AWS WAF token. AWS WAF utilizza i token per il monitoraggio e la verifica delle sessioni dei clienti.

Per informazioni sui token e sulla gestione dei token, vedere. AWS WAF token di richiesta web

Per informazioni sui componenti dell'etichetta descritti qui, vedereRequisiti per la sintassi e la denominazione delle etichette.

Etichetta della sessione del client

L'etichetta `awswaf:managed:token:id:`*`identifier`* contiene un identificatore univoco utilizzato dalla gestione dei AWS WAF token per identificare la sessione client. L'identificatore può cambiare se il client acquisisce un nuovo token, ad esempio dopo aver scartato il token che stava utilizzando.

> **Note**
>
> AWS WAF non riporta i CloudWatch parametri Amazon per questa etichetta.

Etichette di stato dei token: etichetta i prefissi dello spazio dei nomi

Le etichette di stato dei token riportano lo stato del token e le informazioni sulla sfida e sul CAPTCHA in esso contenute.

Ogni etichetta di stato del token inizia con uno dei seguenti prefissi dello spazio dei nomi:

- `awswaf:managed:token:`— Utilizzata per riportare lo stato generale del token e per riportare lo stato delle informazioni sulla sfida del token.
- `awswaf:managed:captcha:`— Utilizzato per riportare lo stato delle informazioni CAPTCHA del token.

Etichette di stato dei token: nomi delle etichette

Dopo il prefisso, il resto dell'etichetta fornisce informazioni dettagliate sullo stato del token:

- `accepted`— Il token di richiesta è presente e contiene quanto segue:
  - Una sfida o una soluzione CAPTCHA valida.

- Una sfida o un timestamp CAPTCHA non scaduti.
- Una specifica di dominio valida per l'ACL web.

Esempio: l'etichetta `awswaf:managed:token:accepted` indica che il token delle richieste Web ha una soluzione di sfida valida, un timestamp della sfida non scaduto e un dominio valido.

- `rejected`— Il token di richiesta è presente ma non soddisfa i criteri di accettazione.

  Oltre all'etichetta rifiutata, la gestione dei token aggiunge uno spazio dei nomi e un nome personalizzati per indicare il motivo.

  - `rejected:not_solved`— Al token manca la sfida o la soluzione CAPTCHA.
  - `rejected:expired`— La sfida o il timestamp CAPTCHA del token sono scaduti, in base ai tempi di immunità del token configurati dall'ACL web.
  - `rejected:domain_mismatch`— Il dominio del token non corrisponde alla configurazione del dominio token dell'ACL Web.
  - `rejected:invalid`— non è AWS WAF riuscito a leggere il token indicato.

  Esempio: `awswaf:managed:captcha:rejected` le etichette `awswaf:managed:captcha:rejected:expired` indicano che la richiesta è stata rifiutata perché il timestamp CAPTCHA nel token ha superato il tempo di immunità del token CAPTCHA configurato nell'ACL web.

- `absent`— La richiesta non ha il token o il gestore del token non è riuscito a leggerlo.

  Esempio: l'etichetta `awswaf:managed:captcha:absent` indica che la richiesta non ha il token.

Etichette Bot Control

Il gruppo di regole gestito da Bot Control genera etichette con il prefisso dello spazio dei nomi `awswaf:managed:aws:bot-control:` seguito dallo spazio dei nomi e dal nome dell'etichetta personalizzati. Il gruppo di regole potrebbe aggiungere più di un'etichetta a una richiesta.

Ogni etichetta riflette i risultati della regola Bot Control:

- `awswaf:managed:aws:bot-control:bot:`— Informazioni sul bot associato alla richiesta.
  - `awswaf:managed:aws:bot-control:bot:name:`*`<name>`*— Il nome del bot, se disponibile, ad esempio i namespace personalizzati e`bot:name:slurp`. `bot:name:googlebot` `bot:name:pocket_parser`

- `awswaf:managed:aws:bot-control:bot:category:<category>`— La categoria del bot, definita, ad esempio AWS WAF, da e. `bot:category:search_engine` `bot:category:content_fetcher`
- `awswaf:managed:aws:bot-control:bot:organization:<organization>`— L'editore del bot, ad esempio,`bot:organization:google`.
- `awswaf:managed:aws:bot-control:bot:verified`— Utilizzato per indicare un bot che si identifica e che Bot Control è stato in grado di verificare. Viene utilizzato per i bot più comuni e può essere utile se combinato con etichette di categoria `bot:category:search_engine` o etichette di nomi come. `bot:name:googlebot`

  > **Note**
  >
  > Bot Control utilizza l'indirizzo IP dell'origine della richiesta web per determinare se un bot è verificato. Non è possibile configurarlo per utilizzare la configurazione IP AWS WAF inoltrata, per ispezionare una fonte di indirizzo IP diversa. Se hai verificato dei bot che eseguono il routing attraverso un proxy o un sistema di bilanciamento del carico, puoi aggiungere una regola che viene eseguita prima del gruppo di regole Bot Control per aiutarti. Configura la tua nuova regola per utilizzare l'indirizzo IP inoltrato e consentire esplicitamente le richieste dei bot verificati. Per informazioni sull'utilizzo degli indirizzi IP inoltrati, consulta. Indirizzo IP inoltrato

- `awswaf:managed:aws:bot-control:bot:user_triggered:verified`— Utilizzato per indicare un bot simile a un bot verificato, ma che potrebbe essere richiamato direttamente dagli utenti finali. Questa categoria di bot viene trattata dalle regole di Bot Control come un bot non verificato.
- `awswaf:managed:aws:bot-control:bot:developer_platform:verified`— Utilizzato per indicare un bot simile a un bot verificato, ma utilizzato dalle piattaforme di sviluppo per lo scripting, ad esempio Google Apps Script. Questa categoria di bot viene trattata dalle regole di Bot Control come un bot non verificato.
- `awswaf:managed:aws:bot-control:bot:unverified`— Utilizzato per indicare un bot che si identifica, quindi può essere denominato e classificato, ma che non pubblica informazioni utilizzabili per verificarne l'identità in modo indipendente. Questi tipi di firme dei bot possono essere falsificate e quindi vengono considerate non verificate.

- `awswaf:managed:aws:bot-control:targeted:<additional-details>` — Utilizzato per etichette specifiche per le protezioni mirate di Bot Control.

- `awswaf:managed:aws:bot-control:signal:<signal-details>`e `awswaf:managed:aws:bot-control:targeted:signal:<signal-details>` — Utilizzato per fornire informazioni aggiuntive sulla richiesta in alcune situazioni.

  Di seguito sono riportati alcuni esempi di etichette di segnale. Questo elenco non è esaustivo:

  - `awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension`— Indica il rilevamento di un'estensione del browser che facilita l'automazione, come Selenium IDE.

    Questa etichetta viene aggiunta ogni volta che un utente ha installato questo tipo di estensione, anche se non la utilizza attivamente. Se implementate una regola di abbinamento delle etichette a tale scopo, tenete presente questa possibilità di falsi positivi nella logica delle regole e nelle impostazioni delle azioni. Ad esempio, è possibile utilizzare un'CAPTCHAazione al posto di Block o combinare questa corrispondenza di etichette con altre corrispondenze di etichette, per aumentare la fiducia nell'utilizzo dell'automazione.
  - `awswaf:managed:aws:bot-control:signal:automated_browser`— Indica che la richiesta contiene indicatori che indicano che il browser del client potrebbe essere automatizzato.
  - `awswaf:managed:aws:bot-control:targeted:signal:automated_browser`— Indica che il AWS WAF token della richiesta contiene indicatori che indicano che il browser del client potrebbe essere automatizzato.

È possibile recuperare tutte le etichette per un gruppo di regole tramite l'API `DescribeManagedRuleGroup` chiamando. Le etichette sono elencate nella `AvailableLabels` proprietà nella risposta.

Il gruppo di regole gestito da Bot Control applica le etichette a un set di bot verificabili che sono comunemente consentiti. Il gruppo di regole non blocca questi bot verificati. Se lo desideri, puoi bloccarli o un sottoinsieme di essi scrivendo una regola personalizzata che utilizza le etichette applicate dal gruppo di regole gestito da Bot Control. Per ulteriori informazioni su questo argomento ed esempi, consultaAWS WAF Controllo dei bot.

Elenco delle regole di Bot Control

Questa sezione elenca le regole di Bot Control.

> **Note**
>
> Le informazioni che pubblichiamo per le regole nei gruppi di regole AWS Managed Rules hanno lo scopo di fornirti informazioni sufficienti per utilizzare le regole, senza fornire informazioni che i malintenzionati potrebbero utilizzare per aggirarle. Se hai bisogno di più informazioni di quelle che trovi in questa documentazione, contatta il AWS Support Centro.

Nome regola	Descrizione
`CategoryAdvertising`	Verifica la presenza di bot utilizzati per scopi pubblicitari. Ad esempio, potresti utilizzare servizi pubblicitari di terze parti che devono accedere programmaticamente al tuo sito Web. Regola d'azione, applicata solo ai bot non verificati: Block Etichetta: `awswaf:managed:aws:bot-control:bot:category:advertising` Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichettatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified`
`CategoryArchiver`	Verifica la presenza di bot utilizzati per scopi di archiviazione. Questi bot eseguono la scansione del Web e acquisiscono contenuti allo scopo di creare archivi. Regola d'azione, applicata solo ai bot non verificati: Block

Nome regola	Descrizione
	Etichetta: `awswaf:managed:aws:bot-control:bot:category:archiver` Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichettatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified`
`CategoryContentFetcher`	Verifica la presenza di bot che visitano il sito Web dell'applicazione per conto di un utente, per recuperare contenuti come i feed RSS o per verificare o convalidare i contenuti. Azione della regola, applicata solo ai bot non verificati: Block Etichetta: `awswaf:managed:aws:bot-control:bot:category:content_fetcher` Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichettatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified`

Nome regola	Descrizione
`CategoryEmailClient`	Verifica la presenza di bot che controllano i link contenuti nelle e-mail che rimandano al sito Web dell'applicazione. Ciò può includere bot gestiti da aziende e provider di posta elettroni ca, per verificare i link nelle e-mail e segnalare le e-mail sospette. Regola d'azione, applicata solo ai bot non verificati: Block Etichetta: `awswaf:managed:aws:bot-control:bot:category:email_client` Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichet tatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified`

Nome regola	Descrizione
`CategoryHttpLibrary`	Controlla le richieste generate dai bot dalle librerie HTTP di vari linguaggi di programma zione. Queste possono includere richieste API che l'utente sceglie di consentire o monitorare. Azione della regola, applicata solo ai bot non verificati: Block Etichetta: `awswaf:managed:aws:bot-control:bot:category:http_library` Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichet tatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified`
`CategoryLinkChecker`	Verifica la presenza di bot che controllano la presenza di link interrotti. Regola d'azione, applicata solo ai bot non verificati: Block Etichetta: `awswaf:managed:aws:bot-control:bot:category:link_checker` Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichet tatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified`

Nome regola	Descrizione
`CategoryMiscellaneous`	Verifica la presenza di bot vari che non corrispondono ad altre categorie. Azione della regola, applicata solo ai bot non verificati: Block Etichetta: `awswaf:managed:aws:bot-control:bot:category:miscellaneous` Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichettatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified`
`CategoryMonitoring`	Verifica la presenza di bot utilizzati per scopi di monitoraggio. Ad esempio, potreste utilizzare servizi di monitoraggio dei bot che eseguono periodicamente il ping del sito Web dell'applicazione per monitorare aspetti come le prestazioni e l'operatività. Regola d'azione, applicata solo ai bot non verificati: Block Etichetta: `awswaf:managed:aws:bot-control:bot:category:monitoring` Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichettatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified`

Nome regola	Descrizione
`CategoryScrapingFramework`	Esamina la presenza di bot dai framework di web scraping, utilizzati per automatizzare la scansione e l'estrazione di contenuti dai siti Web. Azione della regola, applicata solo ai bot non verificati: Block Etichetta: `awswaf:managed:aws:bot-control:bot:category:scraping_framework` Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichettatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified`
`CategorySearchEngine`	Esamina la presenza di bot dei motori di ricerca, che eseguono la scansione dei siti Web per indicizzare i contenuti e rendere disponibili le informazioni per i risultati dei motori di ricerca. Regola d'azione, applicata solo ai bot non verificati: Block Etichetta: `awswaf:managed:aws:bot-control:bot:category:search_engine` Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichettatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified`

Nome regola	Descrizione
`CategorySecurity`	Verifica la presenza di bot che scansionano le applicazioni Web alla ricerca di vulnerabilità o che eseguono controlli di sicurezza. Ad esempio, potreste utilizzare un fornitore di sicurezza di terze parti che scansiona, monitora o verifica la sicurezza delle vostre applicazioni web. Regola d'azione, applicata solo ai bot non verificati: Block Etichetta: `awswaf:managed:aws:bot-control:bot:category:security` Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichettatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified`

Nome regola	Descrizione
`CategorySeo`	Verifica la presenza di bot utilizzati per l'ottimizzazione dei motori di ricerca. Ad esempio, potresti utilizzare gli strumenti dei motori di ricerca che eseguono la scansione del tuo sito per aiutarti a migliorare il posizionamento nei motori di ricerca. Regola d'azione, applicata solo ai bot non verificati: Block Etichetta: `awswaf:managed:aws:bot-control:bot:category:seo` Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichettatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified`

Nome regola	Descrizione
`CategorySocialMedia`	Verifica la presenza di bot utilizzati dalle piattaforme di social media per fornire riepilogh i dei contenuti quando gli utenti condividono i tuoi contenuti. Regola d'azione, applicata solo ai bot non verificati: Block Etichetta: `awswaf:managed:aws:bot-control:bot:category:social_media` Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichet tatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified`
`CategoryAI`	Ispeziona i bot di intelligenza artificiale (AI). Operazione delle regole: Block Etichetta: `awswaf:managed:aws:bot-control:bot:category:ai`

Nome regola	Descrizione
`SignalAutomatedBrowser`	Esamina la richiesta di indicatori che indicano che il browser del client potrebbe essere automatizzato. I browser automatici possono essere utilizzati per test o scraping. Ad esempio, è possibile utilizzare questi tipi di browser per monitorare o verificare il sito Web dell'applicazione. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:bot-control:signal:automated_browser`
`SignalKnownBotDataCenter`	Verifica la presenza di indicatori dei data center utilizzati in genere dai bot. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:bot-control:signal:known_bot_data_center`
`SignalNonBrowserUserAgent`	Controlla le stringhe dello user agent che non sembrano provenire da un browser web. Questa categoria può includere richieste API. Operazione delle regole: Block Etichetta: `awswaf:managed:aws:bot-control:signal:non_browser_user_agent`

Nome regola	Descrizione
`TGT_VolumetricIpTokenAbsent`	Esamina 5 o più richieste di un cliente negli ultimi 5 minuti che non includono un token di sfida valido. Per informazioni sui token, consulta. AWS WAF token di richiesta web **Note** È possibile che questa regola corrispon da a una richiesta con un token se nelle richieste dello stesso client mancano recentemente dei token. La soglia applicata da questa regola può variare leggermente a causa della latenza. Questa regola gestisce i token mancanti in modo diverso dall'etichettatura dei token:. `awswaf:managed:token:absent` L'etichettatura dei token etichetta le singole richieste che non dispongono di un token. Questa regola mantiene il conteggio delle richieste a cui manca il token per ogni IP client e confronta i client che superano il limite. Azione della regola, applicata solo ai client che non sono bot verificati: Challenge Etichetta: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:ip:token_absent` Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichet tatura delle regole più l'etichetta. `awswaf:ma`

Nome regola	Descrizione
	`naged:aws:bot-control:bot:verified`

Nome regola	Descrizione
`TGT_VolumetricSession`	Verifica la presenza di un numero anormalmente elevato di richieste da una sessione client in qualsiasi finestra di 5 minuti. La valutazione si basa su un confronto con le linee di base volumetriche standard che continuano a utilizzare i modelli di traffico storici. AWS WAF Questa ispezione si applica solo quando la richiesta web ha un token. I token vengono aggiunti alle richieste dagli SDK di integrazione delle applicazioni e dalle azioni CAPTCHA delle regole e. Challenge Per ulteriori informazioni, consulta AWS WAF token di richiesta web. **Note** L'entrata in vigore di questa regola può richiedere 5 minuti dopo l'attivazione. Bot Control identifica comportamenti anomali nel traffico web confrontando il traffico corrente con le linee di base del traffico calcolate. AWS WAF Regola d'azione, applicata solo ai client che non sono bot verificati: CAPTCHA Etichetta: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:high` Il gruppo di regole applica le seguenti etichette alle richieste di volume medio e inferiore che superano una soglia minima. Per questi livelli,

Nome regola	Descrizione
	la regola non interviene, indipendentemente dal fatto che il client sia verificato: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:medium` e `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:low`. Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichettatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified`

Nome regola	Descrizione
`TGT_SignalAutomatedBrowser`	Ispeziona il token della richiesta alla ricerca di indicatori che il browser del client potrebbe essere automatizzato. Per ulteriori informazioni, consulta Caratteristiche del token. Questa ispezione si applica solo quando la richiesta web ha un token. I token vengono aggiunti alle richieste dagli SDK di integrazione delle applicazioni e dalle azioni CAPTCHA delle regole e. Challenge Per ulteriori informazioni, consulta AWS WAF token di richiesta web. Azione della regola, applicata solo ai client che non sono bot verificati: CAPTCHA Etichetta: `awswaf:managed:aws:bot-control:targeted:signal:automated_browser` Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichettatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified`

Nome regola	Descrizione
`TGT_SignalBrowserInconsistency`	Verifica la presenza di dati di interrogazione del browser non coerenti. Per ulteriori informazioni, consulta Caratteristiche del token. Questa ispezione si applica solo quando la richiesta web ha un token. I token vengono aggiunti alle richieste dagli SDK di integrazione delle applicazioni e dalle azioni CAPTCHA delle regole e. Challenge Per ulteriori informazioni, consulta AWS WAF token di richiesta web. Azione della regola, applicata solo ai client che non sono bot verificati: CAPTCHA Etichetta: `awswaf:managed:aws:bot-control:targeted:signal:browser_inconsistency` Per i bot verificati, il gruppo di regole non esegue alcuna azione, ma aggiunge l'etichet tatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified`

Nome regola	Descrizione
`TGT_TokenReuseIp`	Verifica l'utilizzo di un singolo token tra più di 5 indirizzi IP distinti. **Note** Le soglie applicate da questa regola possono variare leggermente a causa della latenza. Alcune richieste potrebbero superare il limite prima che venga applicata l'azione della regola. Operazione delle regole: Count Etichetta: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:token_reuse:ip`

Nome regola	Descrizione
`TGT_ML_CoordinatedActivityMedium` e `TGT_ML_CoordinatedActivityHigh`	Verifica la presenza di comportamenti anomali coerenti con l'attività distribuita e coordinata dei bot. I livelli delle regole indicano il livello di certezza che un gruppo di richieste partecipa a un attacco coordinato. **Note** Queste regole vengono eseguite solo se il gruppo di regole è configurato per utilizzare l'apprendimento automatico (ML). Per informazioni sulla configura zione di questa scelta, Aggiungere il gruppo di regole gestito da AWS WAF Bot Control all'ACL web consulta. AWS WAF esegue questa ispezione mediante l'analisi dell'apprendimento automatico delle statistiche sul traffico del sito Web. AWS WAF analizza il traffico web ogni pochi minuti e ottimizza l'analisi per il rilevamento di bot a bassa intensità e di lunga durata distribuiti su molti indirizzi IP. Queste regole potrebbero corrispondere per un numero molto limitato di richieste prima di determinare che non è in corso un attacco coordinato. Quindi, se vedi solo una o due partite, i risultati potrebbero essere falsi positivi. Tuttavia, se vedi che molte partite non rispettan o queste regole, probabilmente stai subendo un attacco coordinato.

Nome regola	Descrizione
	Note Queste regole possono richiedere fino a 24 ore per entrare in vigore dopo aver abilitato le regole mirate di Bot Control con l'opzione ML. Bot Control identifica i comportamenti anomali nel traffico web confrontando il traffico corrente con le linee di base del traffico calcolate. AWS WAF AWS WAF calcola le linee di base solo mentre utilizzi le regole mirate di Bot Control con l'opzione ML e possono essere necessarie fino a 24 ore per stabilire linee di base significative. Aggiorniamo periodicamente i nostri modelli di machine learning in base a queste regole, per migliorare le previsioni dei bot. Se noti un cambiamento improvviso e sostanziale nelle previsioni dei bot formulate da queste regole, contatta il tuo account manager o apri una richiesta al AWS Support Center. Azioni basate sulle regole, applicate solo ai client che non sono bot verificati: • Medium: Count • Elevate: Count Etichette: `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:medium` e

Nome regola	Descrizione
	`awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:high` Per i bot verificati, il gruppo di regole non interviene, ma aggiunge l'etichettatura delle regole più l'etichetta. `awswaf:managed:aws:bot-control:bot:verified` Il gruppo di regole aggiunge anche l'etichetta `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low` per indicare un livello di confidenza basso, ma non applica alcuna regola né intraprende alcuna azione per queste richieste.

Distribuzioni per gruppi di regole AWS Managed Rules con versioni

AWS distribuisce le modifiche ai gruppi di regole AWS Managed Rules corrispondenti in tre distribuzioni standard: release candidate, versione statica e versione predefinita. Inoltre, a volte AWS potrebbe essere necessario rilasciare una distribuzione di eccezioni o ripristinare la distribuzione di una versione predefinita.

> **Note**
>
> Questa sezione si applica solo ai gruppi di regole AWS Managed Rules con versione. I gruppi di regole senza versione sono i gruppi di regole IP Reputation, Bot Control, ATP e ACFP.

Registrati per ricevere notifiche di distribuzione

Per ogni implementazione di un gruppo di regole con versioni, AWS fornisce almeno una notifica SNS. In alcuni casi, aggiorniamo anche la descrizione del gruppo di regole gestite in questa guida, il log delle modifiche per i gruppi di regole AWS Managed Rules e la pagina della cronologia dei

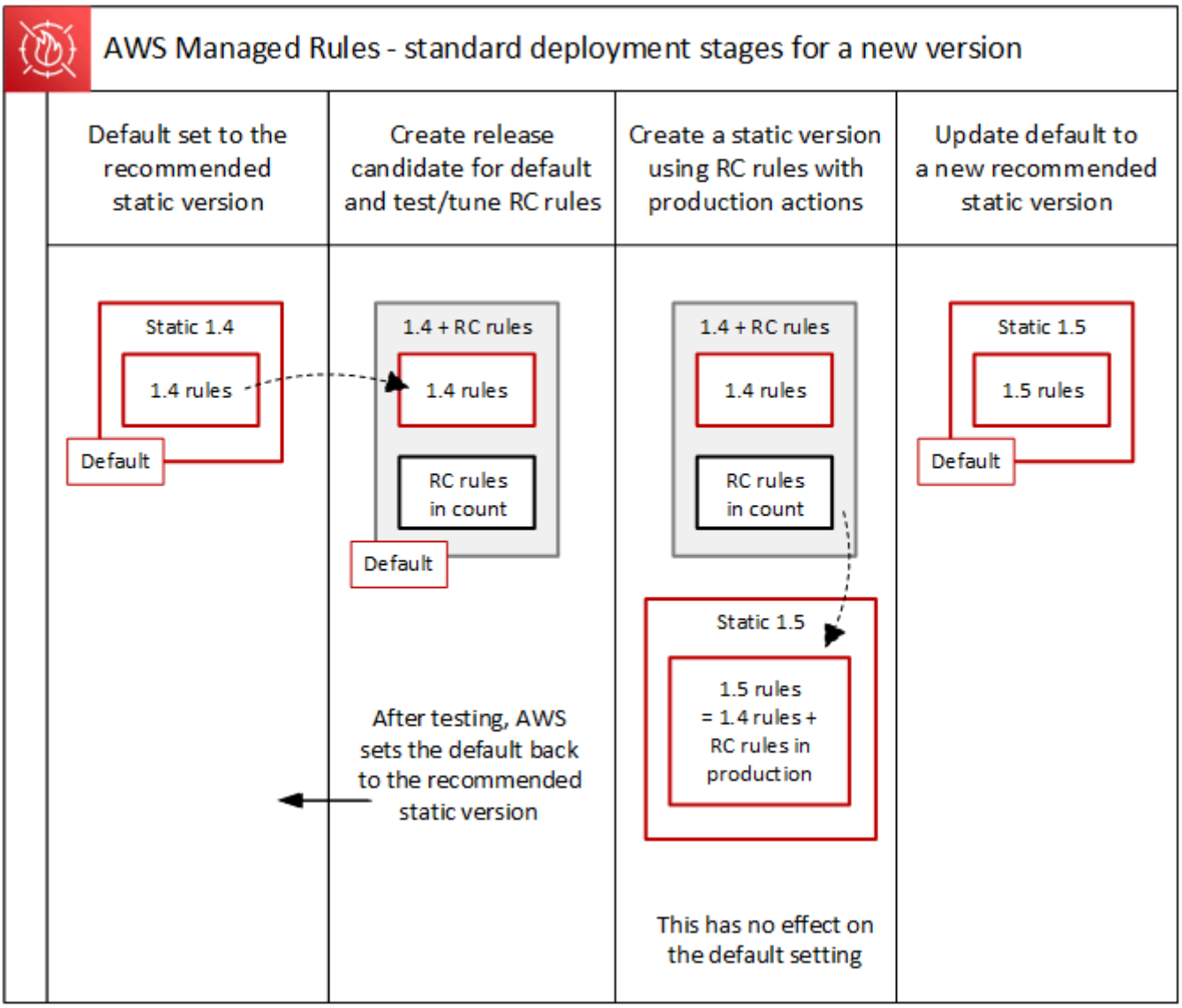
documenti. Per iscriverti alle notifiche, consulta. Ricevere notifiche sulle nuove versioni e sugli aggiornamenti di un gruppo di regole gestito

Argomenti

Panoramica delle implementazioni standard per AWS Managed Rules

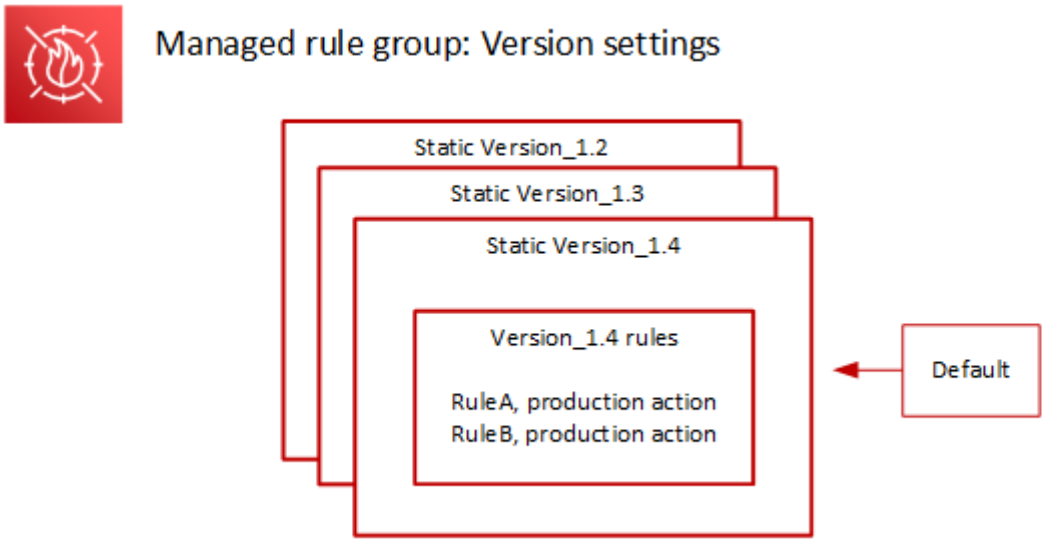
AWS implementa la nuova funzionalità AWS Managed Rules utilizzando tre fasi di distribuzione standard: release candidate, versione statica e versione predefinita.

Il diagramma seguente illustra queste implementazioni standard. Ciascuna di esse è descritta più dettagliatamente nelle sezioni che seguono.



Stati di versione tipici per AWS Managed Rules

Normalmente, un gruppo di regole gestito con versioni ha diverse versioni statiche non scadute e la versione predefinita fa riferimento alla versione statica consigliata. AWS La figura seguente mostra un esempio del tipico set di versioni statiche e dell'impostazione della versione predefinita.



L'azione di produzione per la maggior parte delle regole in una versione statica èBlock, ma potrebbe essere impostata su qualcosa di diverso. Per informazioni dettagliate sulle impostazioni delle azioni delle regole, consulta l'elenco delle regole per ogni gruppo di regole all'indirizzoAWS Elenco dei gruppi di regole di Managed Rules.

Distribuzioni Release Candidate per Managed Rules AWS

Quando AWS dispone di una serie di modifiche alle regole candidate per un gruppo di regole gestito, le verifica in una distribuzione temporanea della release candidate. AWS valuta le regole candidate in modalità count rispetto al traffico di produzione ed esegue le attività di ottimizzazione finale, inclusa l'attenuazione dei falsi positivi. AWS verifica le regole candidate al rilascio in questo modo per tutti i clienti che utilizzano la versione predefinita del gruppo di regole. Le distribuzioni Release Candidate non si applicano ai clienti che utilizzano una versione statica del gruppo di regole.

Se utilizzi la versione predefinita, una distribuzione Release Candidate non altererà il modo in cui il traffico web viene gestito dal gruppo di regole. Potresti notare quanto segue durante il test delle regole candidate:

- Modifica del nome della versione predefinita da `Default (using Version_X.Y)` a`Default (using Version_X.Y_PLUS_RC_COUNT)`.
- Metriche di conteggio aggiuntive in Amazon CloudWatch con `RC_COUNT` i loro nomi. Questi sono generati dalle regole del Release Candidate.

AWS testa una release candidate per circa una settimana, quindi la rimuove e reimposta la versione predefinita alla versione statica attualmente consigliata.

AWS esegue i seguenti passaggi per una distribuzione della release candidate:

1. Crea la release candidate: AWS aggiunge una release candidate basata sulla versione statica attualmente consigliata, che è la versione a cui punta l'impostazione predefinita.

   Il nome della release candidate è il nome della versione statica a cui è stato aggiunto. `_PLUS_RC_COUNT` Ad esempio, se la versione statica attualmente consigliata è`Version_2.1`, la release candidate verrà nominata`Version_2.1_PLUS_RC_COUNT`.

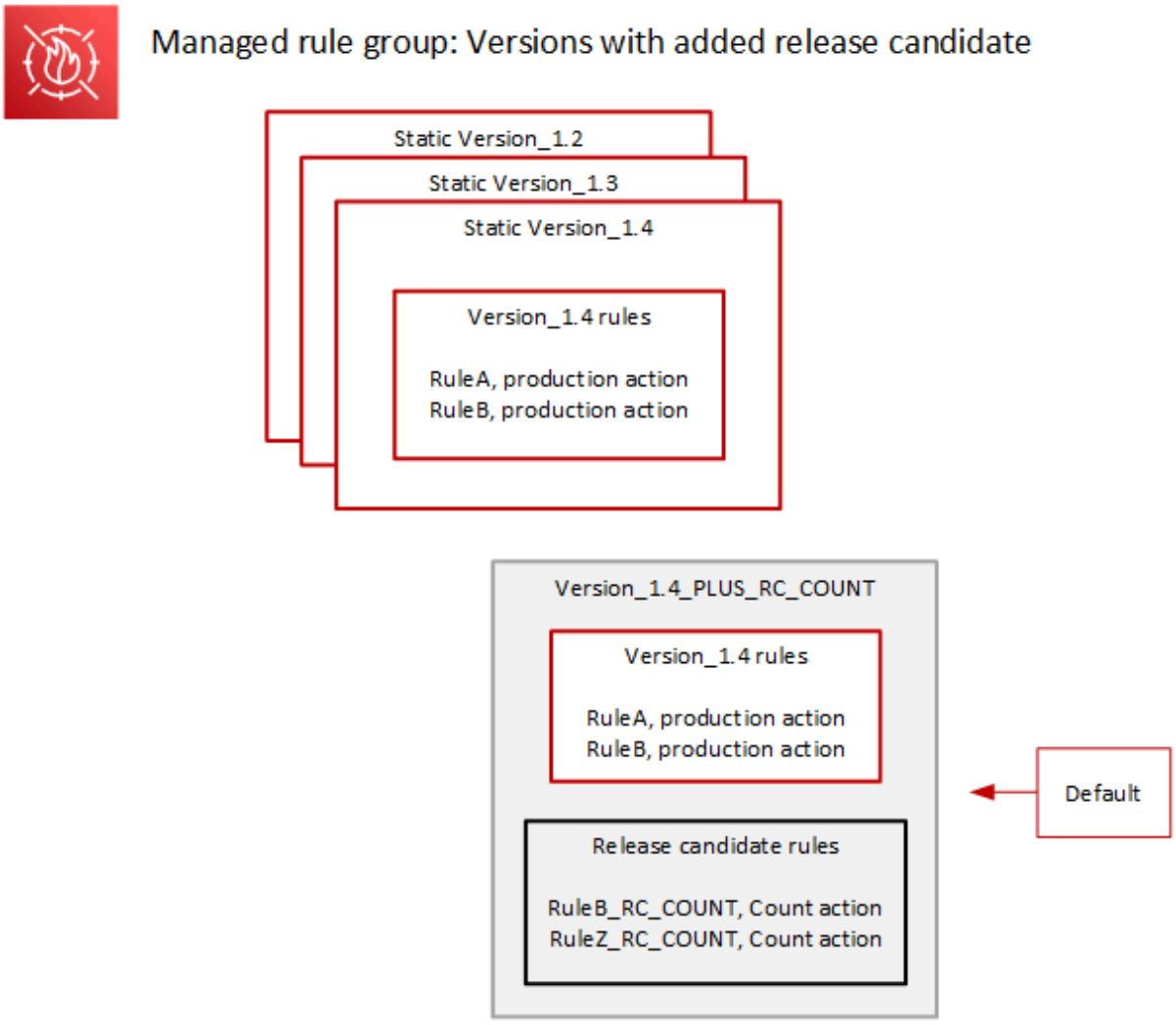
   La release candidate contiene le seguenti regole:

   - Regole copiate esattamente dalla versione statica attualmente consigliata, senza modifiche alle configurazioni delle regole.
   - Proponi nuove regole con regole di azione impostate su Count e con nomi che terminano con. `_RC_COUNT`

     La maggior parte delle regole candidate fornisce miglioramenti proposti alle regole già esistenti nel gruppo di regole. Il nome di ciascuna di queste regole è il nome della regola esistente aggiunto con`_RC_COUNT`.
2. Imposta la versione predefinita sulla release candidate e prova: AWS imposta la versione predefinita in modo che punti alla nuova release candidate, per eseguire test sul traffico di produzione. I test richiedono in genere circa una settimana.

   Vedrai che il nome della versione predefinita cambierà da quello che indica solo la versione statica, ad esempio`Default (using Version_1.4)`, a uno che indica la versione statica più le regole della release candidate, ad esempio`Default (using Version_1.4_PLUS_RC_COUNT)`. Questo schema di denominazione ti consente di identificare la versione statica che stai utilizzando per gestire il traffico web.

   Il diagramma seguente mostra lo stato delle versioni di esempio dei gruppi di regole a questo punto.



Le regole della release candidate sono sempre configurate con Count azioni, quindi non alterano il modo in cui il gruppo di regole gestisce il traffico web.

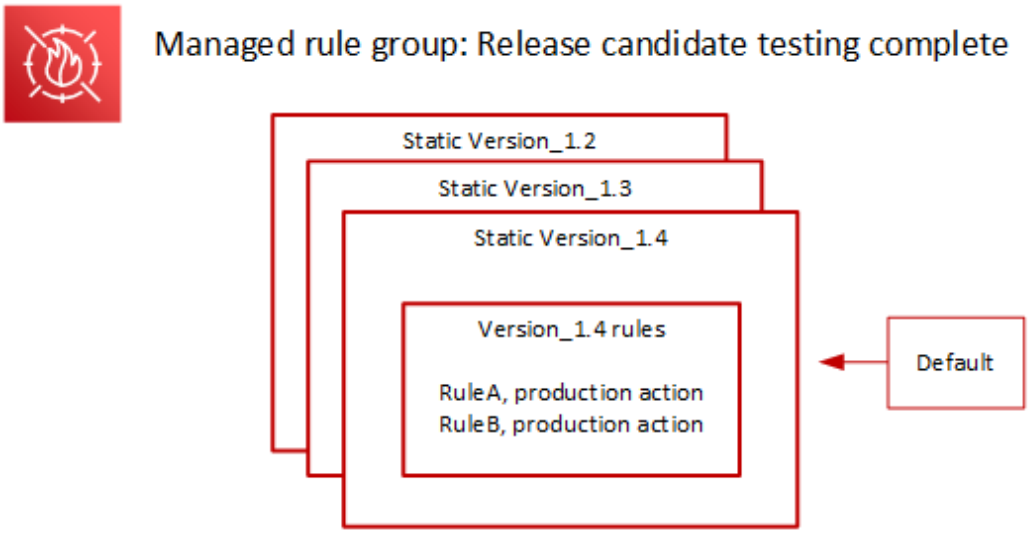
Le regole Release Candidate generano metriche di CloudWatch conteggio di Amazon che AWS vengono utilizzate per verificare il comportamento e identificare i falsi positivi. AWS apporta le modifiche necessarie, per ottimizzare il comportamento delle regole di conteggio delle release candidate.

La versione release candidate non è una versione statica e non è possibile sceglierla dall'elenco delle versioni statiche dei gruppi di regole. È possibile visualizzare solo il nome della versione candidata alla release candidate nella specifica della versione predefinita.

3. Restituisce la versione predefinita alla versione statica consigliata: dopo aver testato le regole della release candidate, AWS riporta la versione predefinita alla versione statica consigliata corrente. L'impostazione predefinita del nome della versione elimina la parte `_PLUS_RC_COUNT` finale e il

gruppo di regole smette di generare metriche di CloudWatch conteggio per le regole della release candidate. Si tratta di una modifica silenziosa e non equivale all'implementazione di un rollback della versione predefinita.

Il diagramma seguente mostra lo stato delle versioni del gruppo di regole di esempio dopo il completamento del test della release candidate.



Tempistica e notifiche

AWS distribuisce le versioni release candidate in base alle esigenze, per testare i miglioramenti apportati a un gruppo di regole.

- SNS: AWS invia una notifica SNS all'inizio della distribuzione. La notifica indica il tempo stimato entro il quale la release candidate verrà testata. Al termine del test, ripristina AWS silenziosamente l'impostazione predefinita della versione statica, senza una seconda notifica.
- Registro delle modifiche: AWS non aggiorna il registro delle modifiche o altre parti di questa guida per questo tipo di distribuzione.

Distribuzioni di versioni statiche per AWS Managed Rules

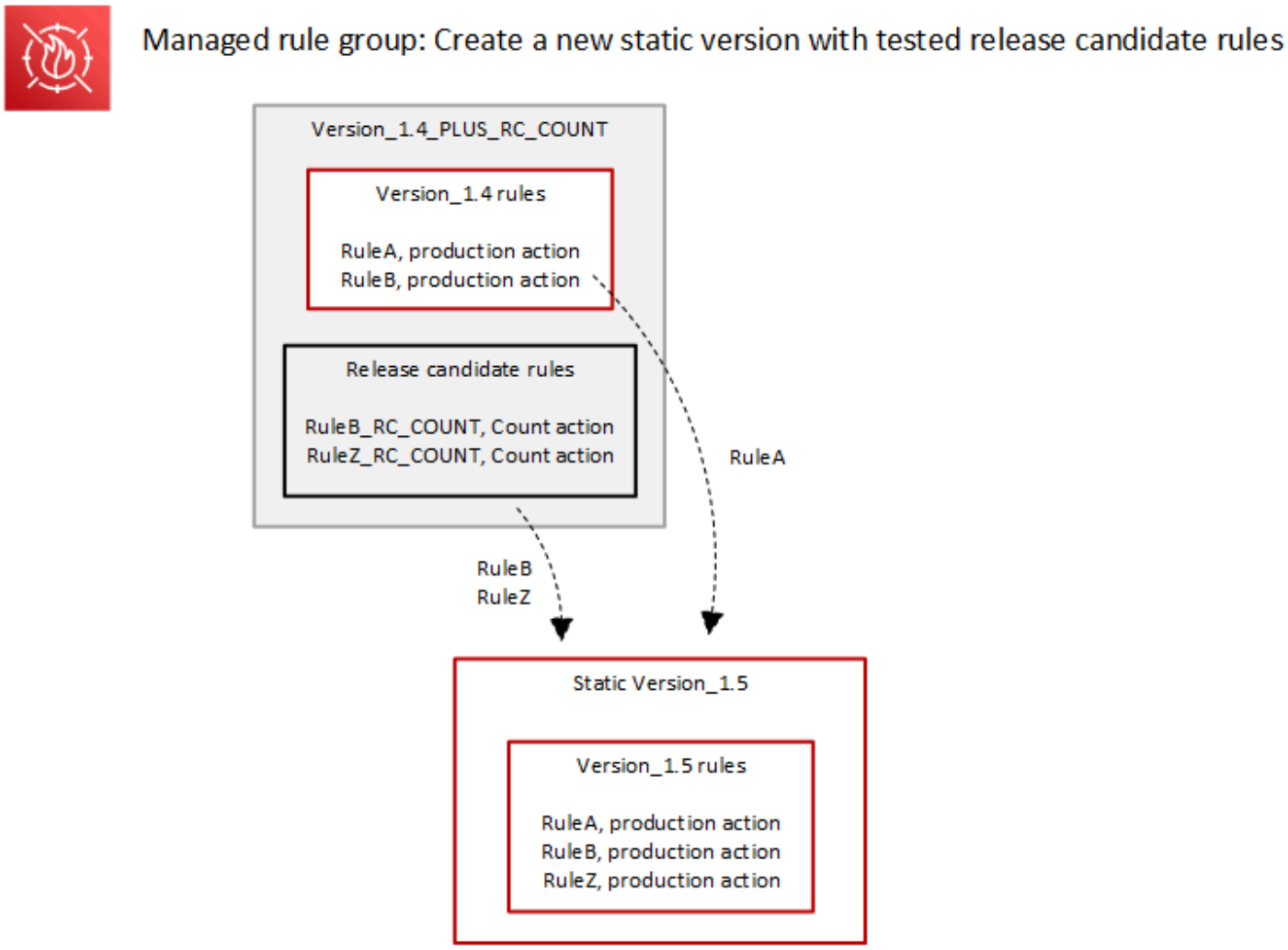
When AWS determina che una release candidate apporta modifiche importanti al gruppo di regole, AWS distribuisce una nuova versione statica per il gruppo di regole basata sulla release candidate. Questa distribuzione non modifica la versione predefinita del gruppo di regole.

La nuova versione statica contiene le seguenti regole della release candidate:

- Regole della versione statica precedente che non hanno un candidato sostitutivo tra le regole della release candidate.
- Regole per la release candidate, con le seguenti modifiche:
  - AWS modifica il nome della regola rimuovendo il suffisso `_RC_COUNT` release candidate.
  - AWS modifica le azioni delle regole dalle Count relative azioni delle regole di produzione.

  Per le regole candidate alla release che sostituiscono le regole esistenti precedenti, queste sostituiscono la funzionalità delle regole precedenti nella nuova versione statica.

Il diagramma seguente illustra la creazione della nuova versione statica dalla release candidate.



Dopo la distribuzione, la nuova versione statica è disponibile per essere testata e utilizzata nelle protezioni, se lo si desidera. Puoi esaminare le azioni e le descrizioni nuove e aggiornate delle regole

negli elenchi di regole del gruppo di regole all'indirizzoAWS Elenco dei gruppi di regole di Managed Rules.

Una versione statica è immutabile dopo la distribuzione e cambia solo AWS alla scadenza. Per informazioni sui cicli di vita delle versioni, consulta. Gestione delle versioni con gruppi di regole gestiti

Tempistica e notifiche

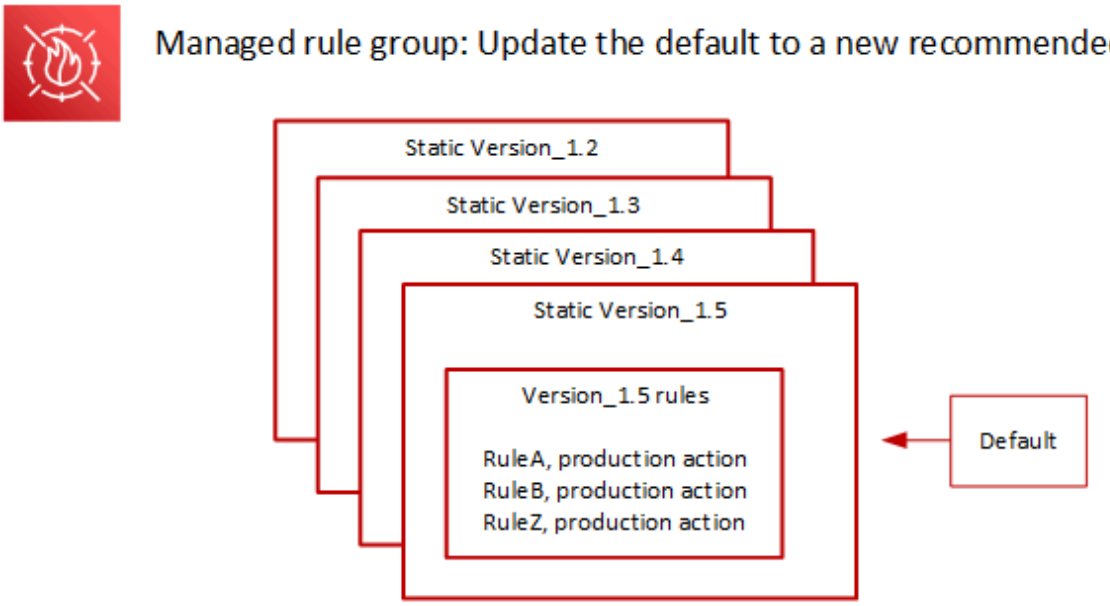
AWS distribuisce una nuova versione statica secondo necessità, per implementare miglioramenti alla funzionalità dei gruppi di regole. La distribuzione di una versione statica non influisce sull'impostazione della versione predefinita.

- SNS: AWS invia una notifica SNS all'inizio della distribuzione.
- Registro delle modifiche: una volta completata la distribuzione ovunque AWS WAF sia disponibile, AWS aggiorna la definizione del gruppo di regole in questa guida secondo necessità, quindi annuncia la versione nel registro delle modifiche del gruppo di regole AWS Managed Rules e nella pagina della cronologia della documentazione.

Distribuzioni di versioni predefinite per AWS Managed Rules

When AWS determina che una nuova versione statica fornisce una protezione migliore per il gruppo di regole rispetto all'impostazione predefinita corrente, AWS aggiorna la versione predefinita alla nuova versione statica. AWS potrebbe rilasciare più versioni statiche prima di promuoverne una alla versione predefinita del gruppo di regole.

Il diagramma seguente mostra lo stato delle versioni di esempio del gruppo di regole dopo lo AWS spostamento dell'impostazione della versione predefinita nella nuova versione statica.



Prima di implementare questa modifica alla versione predefinita, AWS fornisce notifiche in modo da poter testare e prepararsi per le modifiche imminenti. Se utilizzi la versione predefinita, non puoi intraprendere alcuna azione e mantenerla invariata durante l'aggiornamento. Se invece desideri ritardare il passaggio alla nuova versione, prima dell'inizio pianificato della distribuzione della versione predefinita, puoi configurare in modo esplicito il tuo gruppo di regole per utilizzare la versione statica su cui è impostata quella predefinita.

Tempistica e notifiche

AWS aggiorna la versione predefinita quando consiglia una versione statica diversa per il gruppo di regole rispetto a quella attualmente in uso.

- SNS: AWS invia una notifica SNS almeno una settimana prima del giorno di distribuzione previsto e poi un'altra il giorno della distribuzione, all'inizio della distribuzione. Ogni notifica include il nome del gruppo di regole, la versione statica a cui viene aggiornata la versione predefinita, la data di distribuzione e la tempistica pianificata della distribuzione per ogni AWS regione in cui viene eseguito l'aggiornamento.
- Registro delle modifiche: AWS non aggiorna il registro delle modifiche o altre parti di questa guida per questo tipo di distribuzione.

Distribuzioni di eccezioni per Managed Rules AWS

AWS potrebbe aggirare le fasi di distribuzione standard per distribuire rapidamente aggiornamenti che risolvono i rischi critici per la sicurezza. Una distribuzione eccezionale potrebbe coinvolgere qualsiasi tipo di distribuzione standard e potrebbe essere implementata rapidamente in tutte le AWS regioni.

AWS fornisce il maggior numero possibile di notifiche anticipate per le distribuzioni di eccezioni.

Tempistica e notifiche

AWS esegue distribuzioni di eccezioni solo quando richiesto.

- SNS: AWS invia una notifica SNS il prima possibile del giorno di implementazione previsto e poi un'altra all'inizio della distribuzione. Ogni notifica include il nome del gruppo di regole, la modifica apportata e la data di implementazione.
- Registro delle modifiche: se la distribuzione riguarda una versione statica, una volta completata la distribuzione ovunque AWS WAF sia disponibile, AWS aggiorna la definizione del gruppo di regole in questa guida secondo necessità, quindi annuncia la versione nel registro delle modifiche del gruppo di regole AWS Managed Rules e nella pagina della cronologia della documentazione.

Rollback di distribuzione predefiniti per AWS Managed Rules

In determinate condizioni, AWS potrebbe ripristinare la versione predefinita all'impostazione precedente. Un rollback richiede in genere meno di dieci minuti per tutte le AWS regioni.

AWS esegue un rollback solo per mitigare un problema significativo in una versione statica, ad esempio un livello inaccettabilmente elevato di falsi positivi.

Dopo il ripristino dell'impostazione della versione predefinita, AWS accelera sia la scadenza della versione statica che presenta il problema sia il rilascio di una nuova versione statica per risolvere il problema.

Tempistica e notifiche

AWS esegue i rollback delle versioni predefinite solo quando richiesto.

- SNS: AWS invia una singola notifica SNS al momento del rollback. La notifica include il nome del gruppo di regole, la versione su cui viene impostata la versione predefinita e la data di distribuzione. Questo tipo di distribuzione è molto rapido, quindi la notifica non fornisce informazioni sulla tempistica per le regioni.

- Registro delle modifiche: AWS non aggiorna il registro delle modifiche o altre parti di questa guida per questo tipo di distribuzione.

AWS Esclusione di responsabilità su Managed Rules

AWS Le Managed Rules sono progettate per proteggerti dalle minacce web più comuni. Se utilizzati in conformità con la documentazione, i gruppi di regole AWS Managed Rules aggiungono un altro livello di sicurezza per le applicazioni. Tuttavia, i gruppi di regole AWS Managed Rules non sono intesi come sostituti delle responsabilità in materia di sicurezza, che sono determinate dalle AWS risorse selezionate. Fai riferimento al modello di responsabilità condivisa per assicurarti che le tue risorse AWS siano adeguatamente protette.

AWS Registro delle modifiche di Managed Rules

Questa sezione elenca le modifiche apportate alle AWS Managed Rules AWS WAF dalla loro pubblicazione a novembre 2019.

> **Note**
>
> Questo registro delle modifiche riporta le modifiche alle regole e ai gruppi di regole in AWS Managed Rules for. AWS WAF
> Per ilGruppi di regole Reputazione IP, questo changelog riporta le modifiche alle regole e al gruppo di regole e riporta modifiche significative alle fonti degli elenchi di indirizzi IP utilizzati dalle regole. Non riporta le modifiche agli elenchi di indirizzi IP stessi, a causa della natura dinamica di tali elenchi. Se hai domande sugli elenchi di indirizzi IP, contatta il tuo account manager o apri una richiesta presso AWS Support Center.

Gruppo di regole e regole	Descrizione	Data
Gruppo di regole gestito con Amazon IP Reputation List • `AWSManagedIPReputationList`	Sono state aggiornate le fonti dell'elenco di reputazione IP per migliorare l'identificazione degli indirizzi che svolgono attivamente attività dannose e ridurre i falsi positivi.	2024-03-13

Gruppo di regole e regole	Descrizione	Data
	Questo aggiornamento non prevede una nuova versione perché questo gruppo di regole non dispone di versioni.	
Input non validi noti: gruppo di regole gestito	Rilasciata la versione statica 1.21 di questo gruppo di regole. Sono state aggiunte firme per migliorare il rilevamento e ridurre i falsi positivi.	2023-12-16
Input non validi noti: gruppo di regole gestito • `ExploitablePaths_URIPATH`	È stata rilasciata la versione statica 1.20 di questo gruppo di regole. È stata aggiornata la `ExploitablePaths_URIPATH` regola per aggiungere il rilevamento delle richieste che corrispondono alla vulnerabilità di autorizzazione impropria CVE-2023-22518 di Atlassian Confluence. Questa vulnerabilità riguarda tutte le versioni di Confluence Data Center and Server. Per ulteriori informazioni, consulta NIST: National Vulnerability Database: CVE-2023-22518 Detail.	2023-12-14

Gruppo di regole e regole	Descrizione	Data
Gruppo di regole gestito dal Core Rule Set (CRS) • `CrossSiteScripting*`	Rilasciata la versione statica 1.11 di questo gruppo di regole. Sono state aggiunte firme a tutte le regole di cross-sit e scripting per migliorare il rilevamento e ridurre i falsi positivi.	2023-12-06
AWS WAF Gruppo di regole Bot Control • Nuova etichetta: `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low`	È stata aggiunta l'etichetta Coordinated Activity Low alle etichette del livello di protezione mirato del gruppo di regole. Questa etichetta non è associata ad alcuna regola. Questa etichettatura si aggiunge alle regole e alle etichette di livello medio e alto.	2023-12-05
Etichette Bot Control • Etichetta: `awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension`	È stata aggiunta un'etichetta di segnale al gruppo di regole che indica il rilevamento di un'estensione del browser che facilita l'automazione. Questa etichetta non è specifica per una singola regola.	2023-11-14
Gruppo di regole gestito dal Core Rule Set (CRS) • `EC2MetaDataSSRF_QUERYARGUMENTS`	Rilasciata la versione statica 1.10 di questo gruppo di regole. È stata aggiornata una regola per migliorare il rilevamento e ridurre i falsi positivi.	2023-11-02

Gruppo di regole e regole	Descrizione	Data
Gruppo di regole gestito dal Core Rule Set (CRS) • EC2MetaDataSSRF_BODY • EC2MetaDataSSRF_COOKIE • EC2MetaDataSSRF_URIPATH • EC2MetaDataSSRF_QUERYARGUMENTS	Rilasciata la versione statica 1.9 di questo gruppo di regole. Regole aggiornate per migliorare il rilevamento e ridurre i falsi positivi.	2023-10-30
gruppo di regole gestito dal sistema operativo POSIX • UNIXShellCommandsVariables_QUERYARGUMENTS	È stata rilasciata la versione statica 2.1 di questo gruppo di regole. È stata aggiornata la regola degli argomenti della query per migliorare il rilevamento.	2023-10-12

Gruppo di regole e regole	Descrizione	Data
Gruppo di regole gestito dal Core Rule Set (CRS) • `GenericLFI_QUERYARGUMENTS` • `GenericLFI_URIPATH` • `RestrictedExtensions_URIPATH` • `RestrictedExtensions_QUERYARGUMENTS`	Rilasciata la versione statica 1.8 di questo gruppo di regole. Regole aggiornate per migliorare il rilevamento.	2023-10-11

Gruppo di regole e regole	Descrizione	Data
Input non validi noti: gruppo di regole gestito • `ExploitablePaths_URIPATH`	Distribuzione delle eccezioni : rilasciata la versione statica 1.19 di questo gruppo di regole. È stata aggiornata la versione predefinita per utilizzare la versione 1.19. È stata aggiornata la `ExploitablePaths_URIPATH` regola per aggiungere il rilevamento delle richieste corrispondenti alla vulnerabilità Privilege Escalation CVE-2023-22515 di Atlassian Confluence. Questa vulnerabilità riguarda alcune versioni di Atlassian Confluence. Per ulteriori informazioni, vedere NIST: National Vulnerability Database: CVE-2023-22515 Detail e Atlassian Support: FAQ for CVE-2023-22515. Per informazioni su Distribuzioni di eccezioni per Managed Rules AWS questo tipo di distribuzione, consulta.	2023-10-04

Gruppo di regole e regole	Descrizione	Data
Input non validi noti: gruppo di regole gestito • `Host_localhost_HEADER` • `Log4J*` • `JavaDeserialization*`	Distribuzione delle eccezioni : rilasciata la versione statica 1.18 di questo gruppo di regole. Questa è una rapida implementazione di questa versione statica per consentire la creazione e il lancio della versione 1.19. Sono state aggiornate la `Host_localhost_HEADER` regola e tutte le regole di deserializzazione di Log4J e Java per un migliore rilevamento. Per informazioni su questo tipo di distribuzione, consulta. Distribuzioni di eccezioni per Managed Rules AWS	2023-10-04

Gruppo di regole e regole	Descrizione	Data
AWS WAF Gruppo di regole Bot Control • `TGT_TokenReuseIp` • `TGT_ML_CoordinatedActivityMedium` • `TGT_ML_CoordinatedActivityHigh`	Aggiunte regole al gruppo di regole con azione. Count La regola IP di riutilizzo dei token rileva e conta la condivisione dei token tra gli indirizzi IP. Le regole di attività coordinate utilizzano l'analisi automatizzata di apprendimento automatico (ML) del traffico del sito Web per rilevare le attività relative ai bot. Nella configurazione del gruppo di regole, puoi disattivare l'uso del machine learning. Con questa versione, i clienti che attualmente utilizzano il livello di protezione mirato possono optare per l'uso del machine learning. La disattivazione disabilita le regole delle attività coordinate.	2023-09-06
AWS WAF Gruppo di regole Bot Control • `CategoryAI`	Aggiunta la regola al gruppo di regole`CategoryAI` .	2023-08-30

Gruppo di regole e regole	Descrizione	Data
Gruppo di regole gestito dal Core Rule Set (CRS) • `RestrictedExtensions_URIPATH` • `RestrictedExtensions_QUERYARGUMENTS` • `EC2MetaDataSSRF_COOKIE` • `EC2MetaDataSSRF_QUERYARGUMENTS` • `EC2MetaDataSSRF_BODY` • `EC2MetaDataSSRF_URIPATH`	È stata rilasciata la versione statica 1.7 di questo gruppo di regole. Estensioni limitate e regole SSRF dei metadati EC2 aggiornate per migliorare il rilevamento e ridurre i falsi positivi.	2023-07-26
AWS WAF Gruppo di regole per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control Tutte le regole in un nuovo gruppo di regole	Aggiunto il gruppo di regole`AWSManagedRulesACFPRuleSet` .	2023-06-13

Gruppo di regole e regole	Descrizione	Data
Gruppo di regole gestito dal sistema operativo Linux • LFI_HEADER • LFI_URIPATH • LFI_QUERYSTRING	Rilasciata la versione statica 2.2 di questo gruppo di regole. Sono state aggiunte firme per migliorare il rilevamento.	2023-05-22
Gruppo di regole gestito dal Core Rule Set (CRS) • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	Rilasciata la versione statica 1.6 di questo gruppo di regole. Aggiornamento delle regole di cross-site scripting (XSS) e delle estensioni limitate per migliorare il rilevamento e ridurre i falsi positivi.	2023-04-28

Gruppo di regole e regole	Descrizione	Data
Gruppo di regole gestito dall'applicazione PHP • Aggiornato `PHPHighRiskMethodsVariables_BODY` • Rimosso `PHPHighRiskMethodsVariables_QUERYARGUMENTS` • Aggiunto `PHPHighRiskMethodsVariables_QUERYSTRING` • Aggiunto `PHPHighRiskMethodsVariables_HEADER`	È stata rilasciata la versione statica 2.0 di questo gruppo di regole. Sono state aggiunte firme per migliorare il rilevamento in tutte le regole. La regola è stata sostituita `PHPHighRiskMethodsVariables_QUERYARGUMENTS` con `PHPHighRiskMethodsVariables_QUERYSTRING`, che controlla l'intera stringa di query anziché solo gli argomenti della query. È stata aggiunta la regola `PHPHighRiskMethodsVariables_HEADER` per espandere la copertura in modo da includere tutte le intestazioni. Sono state aggiornate le seguenti etichette per allinearle all'etichettatura standard delle AWS Managed Rules: • Vecchio nome: `PHPHighRiskMethodsVariables_BODY` Nuovo nome: `PHPHighRiskMethodsVariables_Body`	2023-02-27

Gruppo di regole e regole	Descrizione	Data
	• Vecchio nome: `PHPHighRiskMethodsVariables_QUERYARGUMENTS` Nuovo nome: `PHPHighRiskMethodsVariables_QueryString`	
AWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi • `VolumetricIpFailedLoginResponseHigh` • `VolumetricSessionFailedLoginResponseHigh`	Sono state aggiunte regole di ispezione della risposta di accesso da utilizzare con CloudFront distribuzioni Amazon protette. Queste regole possono bloccare nuovi tentativi di accesso da indirizzi IP e sessioni client che recentemente sono stati all'origine di troppi tentativi di accesso falliti.	15/02/23
Gruppo di regole gestito dal Core Rule Set (CRS) • `NoUserAgent_HEADER` • `CrossSiteScripting_COOKIE` • `CrossSiteScripting_QUERYARGUMENTS` • `CrossSiteScripting_BODY` • `CrossSiteScripting_URIPATH`	Rilasciata la versione statica 1.5 di questo gruppo di regole. Filtri Cross Site Scripting (XSS) aggiornati per migliorare il rilevamento.	2023-01-25

Gruppo di regole e regole	Descrizione	Data
Gruppo di regole gestito dal sistema operativo Linux • `LFI_COOKIE` - rimosso • `LFI_HEADER` - aggiunto • `LFI_URIPATH` • `LFI_QUERYSTRING`	È stata rilasciata la versione statica 2.1 di questo gruppo di regole. Ha rimosso la regola `LFI_COOKIE` e la relativa etichetta `awswaf:managed:aws:linux-os:LFI_Cookie` e le ha sostituite con la nuova regola `LFI_HEADER` e la relativa etichetta `awswaf:managed:aws:linux-os:LFI_Header`. Questa modifica estende l'ispezione a più intestazioni. Sono state aggiunte trasformazioni e firme di testo a tutte le regole per migliorare il rilevamento.	15-12-12 2022.

Gruppo di regole e regole	Descrizione	Data
Gruppo di regole gestito dal Core Rule Set (CRS) • NoUserAgent_HEADER • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	Rilasciata la versione statica 1.4 di questo gruppo di regole. Aggiunta una trasformazione del testo per NoUserAgent_HEADER rimuovere tutti i byte nulli. Sono stati aggiornati i filtri nelle regole di cross-site scripting per migliorare il rilevamento.	2022-12-05

Gruppo di regole e regole	Descrizione	Data
Input non validi noti: gruppo di regole gestito • `JavaDeserializationRCE_BODY` • `JavaDeserializationRCE_URIPATH` • `JavaDeserializationRCE_HEADER` • `JavaDeserializationRCE_QUERYSTRING` • `Host_localhost_HEADER`	Rilasciata la versione statica 1.17 di questo gruppo di regole. Sono state aggiornate le regole di deserializzazione Java per aggiungere il rilevamento delle richieste corrispondenti ad Apache CVE-2022-42889, una vulnerabilità di esecuzione di codice in modalità remota (RCE) nelle versioni di Apache Commons Text precedenti alla 1.10.0. Per ulteriori informazioni, vedere NIST: National Vulnerability Database: CVE-2022-42889 Detail e CVE-2022-42889: Apache Commons Text precedente alla 1.10.0 consente RCE se applicato a input non attendibili a causa di impostazioni di interpolazione non sicure. Rilevamento migliorato in. `Host_localhost_HEADER`	2022-10-20

Gruppo di regole e regole	Descrizione	Data
Input non validi noti: gruppo di regole gestito • `Log4JRCE_HEADER` • `Log4JRCE_QUERYSTRING` • `Log4JRCE_URIPATH` • `Log4JRCE_BODY`	Rilasciata la versione statica 1.16 di questo gruppo di regole. Sono stati rimossi i falsi positivi AWS identificati nella versione 1.15.	2022-10-05
gruppo di regole gestito dal sistema operativo POSIX Gruppo di regole gestito dall'applicazione PHP WordPress gruppo di regole gestito dall'applicazione	Sono stati corretti i nomi delle etichette documentati.	2022-09-19
Gruppi di regole Reputazione IP • `AWSManagedIPDDoSList`	Questa modifica non modifica il modo in cui il gruppo di regole gestisce il traffico web. È stata aggiunta una nuova regola che prevede Count l'ispezione degli indirizzi IP coinvolti attivamente in attività DDoS, secondo l'intelligence sulle minacce di Amazon.	30/08/2022

Gruppo di regole e regole	Descrizione	Data
Input non validi noti: gruppo di regole gestito • Log4JRCE • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URIPATH • Log4JRCE_BODY • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URIPATH • JavaDeserializationRCE_QUERYSTRING • Host_localhost_HEADER • PROPFIND_METHOD	Rilasciata la versione statica 1.15 di questo gruppo di regole. Rimossa Log4JRCE e sostituita con Log4JRCE_HEADER ,, e Log4JRCE_QUERYSTRING Log4JRCE_URI Log4JRCE_BODY , per un monitoraggio e una gestione più granulari dei falsi positivi. Sono state aggiunte firme per migliorare il rilevamento e il blocco di tutti PROPFIND_METHOD JavaDeserialization RCE* e le regole. Log4JRCE* Etichette aggiornate per correggere l'uso delle maiuscole in Host_localhost_HEADER e in tutte le JavaDeserializationRCE* regole. È stata corretta la descrizione di. JavaDeserializationRCE_HEADER	2022-08-22

Gruppo di regole e regole	Descrizione	Data
AWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi • `UnsupportedCognitoIDP`	È stata aggiunta una regola per impedire l'uso del gruppo di regole gestite per la prevenzione dell'acquisizione di account per il traffico web del pool di utenti di Amazon Cognito.	11/08/2022
Gruppo di regole gestito dal Core Rule Set (CRS)	AWS ha una scadenza programmata per le versioni `Version_1.2` e il gruppo `Version_2.0` di regole. Le versioni scadranno il 9 settembre 2022. Per informazioni sulla scadenza della versione, consultaGestione delle versioni con gruppi di regole gestiti.	2022-06-09
Gruppo di regole gestito dal Core Rule Set (CRS) • `GenericLFI_URIPATH` `GenericRFI_URIPATH`	È stata rilasciata la versione 1.3 di questo gruppo di regole. Questa versione aggiorna le firme delle partite nelle regole `GenericLFI_URIPATH` e `GenericRFI_URIPATH` per migliorarne il rilevamento.	24 maggio 2022
AWS WAF Gruppo di regole Bot Control • `CategoryEmailClient`	Aggiunta la regola al gruppo di regole`CategoryEmailClient` .	2022-04-06

Gruppo di regole e regole	Descrizione	Data
Input non validi noti: gruppo di regole gestito • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URI • JavaDeserializationRCE_QUERYSTRING	È stata rilasciata la versione 1.14 di questo gruppo di regole. Le quattro JavaDeserializtionRCE regole vengono spostate in Block modalità.	2022-03-31
Input non validi noti: gruppo di regole gestito • JavaDeserializationRCE_HEADER_RC_COUNT • JavaDeserializationRCE_BODY_RC_COUNT • JavaDeserializationRCE_URI_RC_COUNT • JavaDeserializationRCE_QUERYSTRING_RC_COUNT	È stata rilasciata la versione 1.13 di questo gruppo di regole. Aggiornata la trasformazione del testo per le vulnerabilità RCE di Spring Core e Cloud Function. Queste regole sono in modalità conteggio per raccogliere metriche e valutare i modelli corrispondenti. L'etichetta può essere utilizzata per bloccare le richieste in una regola personalizzata. Verrà distribuita una versione successiva con queste regole in modalità a blocchi.	2022-03-31

Gruppo di regole e regole	Descrizione	Data
Input non validi noti: gruppo di regole gestito • 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	È stata rilasciata la versione 1.12 di questo gruppo di regole. Aggiunte firme per le vulnerabilità RCE di Spring Core e Cloud Function. Queste regole sono in modalità conteggio per raccogliere metriche e valutare i modelli corrispondenti. L'etichetta può essere utilizzata per bloccare le richieste in una regola personalizzata. Verrà distribuita una versione successiva con queste regole in modalità a blocchi. Ha rimosso le regole Log4JRCE_HEADER , Log4JRCE_QUERYSTRING Log4JRCE_URI , Log4JRCE_BODY e le ha sostituite con la regola Log4JRCE.	2022-03-30
Gruppi di regole Reputazione IP • AWSManagedReconnaissanceList	È stata aggiornata la AWSManagedReconnaissanceList regola per modificare l'azione da conteggio a blocco.	15/02/2022

Gruppo di regole e regole	Descrizione	Data
AWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi Tutte le regole nel nuovo gruppo di regole	Aggiunto il gruppo di regole`AWSManagedRulesATPRuleSet` .	11/02/2022
Input non validi noti: gruppo di regole gestito - `Log4JRCE` - `Log4JRCE_HEADER` - `Log4JRCE_QUERYSTRING` - `Log4JRCE_URI` - `Log4JRCE_BODY`	È stata rilasciata la versione 1.9 di questo gruppo di regole. È stata rimossa la regola `Log4JRCE` e l'ha sostituita con le regole `Log4JRCE_HEADER` `Log4JRCE_QUERYSTRING` `Log4JRCE_URI` ,`Log4JRCE_BODY` , e, per una maggiore flessibilità nell'uso di questa funzionalità. Sono state aggiunte firme per migliorare il rilevamento e il blocco.	28/01/2022

Gruppo di regole e regole	Descrizione	Data
Core rule set (CRS) • `CrossSiteScripting_URIPATH` • `CrossSiteScripting_BODY` • `CrossSiteScripting_QUERYARGUMENTS` • `CrossSiteScripting_COOKIE`	È stata rilasciata la versione 2.0 di questo gruppo di regole. Per queste regole, sono state ottimizzate le firme di rilevamento per ridurre i falsi positivi. Ha sostituito la trasformazione del `URL_DECODE` testo con la trasformazione a doppio `URL_DECODE_UNI` testo. È stata aggiunta la trasformazione `HTML_ENTITY_DECODE` del testo.	10/01/2022
Core rule set (CRS) • `RestrictedExtensions_URIPATH` • `RestrictedExtensions_QUERYARGUMENTS`	Come parte del rilascio della versione 2.0 di questo gruppo di regole, è stata aggiunta la trasformazione del testo. `URL_DECODE_UNI` È stata rimossa la trasformazione `URL_DECODE` del testo da`RestrictedExtensions_URIPATH` .	10/01/2022

Gruppo di regole e regole	Descrizione	Data
Database SQL • SQLi_BODY • SQLi_QUERYARGUMENTS • SQLi_COOKIE • SQLi_URIPATH • SQLiExtendedPatterns_BODY • SQLiExtendedPatterns_QUERYARGUMENTS	È stata rilasciata la versione 2.0 di questo gruppo di regole. Ha sostituito la trasformazione del URL_DECODE testo con la trasformazione a doppio URL_DECODE_UNI testo e ha aggiunto la trasformazione del COMPRESS_WHITE_SPACE testo. Sono state aggiunte altre firme di rilevamento a. SQLiExtendedPatterns_QUERYARGUMENTS È stata aggiunta l'ispezione JSON a. SQLi_BODY È stata aggiunta la regolaSQLiExtendedPatterns_BODY . È stata rimossa la regolaSQLi_URIPATH .	2022-01-10
Known bad inputs • Log4JRCE	È stata rilasciata la versione 1.8 della regola Log4JRCE per migliorare l'ispezione delle intestazioni e i criteri di corrispondenza.	17/12/2021

Gruppo di regole e regole	Descrizione	Data
Known bad inputs • `Log4JRCE`	È stata rilasciata la versione 1.4 della regola `Log4JRCE` per ottimizzare i criteri di abbinamento e controllare gli header aggiuntivi. Rilasciata la versione 1.5 per ottimizzare i criteri di abbinamento.	2021-12-11
Known bad inputs • `Log4JRCE` • `BadAuthToken_COOKIE_AUTHORIZATION`	Aggiunta la `Log4JRCE` versione 1.2 della regola in risposta al problema di sicurezza recentemente divulgato all'interno di Log4j. Per informazioni, vedere CVE-2021-44228. Questa regola controlla i percorsi URI comuni, le stringhe di query, i primi 8 KB del corpo della richiesta e le intestazioni comuni. La regola utilizza trasformazioni a doppio testo. `URL_DECODE_UNI` È stata rilasciata la versione 1.3 di `Log4JRCE` per ottimizzare i criteri di corrispondenza e controllare le intestazioni aggiuntive. Rimossa la regola. `BadAuthToken_COOKIE_AUTHORIZATION`	2021-12-10

La tabella seguente elenca le modifiche precedenti a dicembre 2021.

Gruppo di regole e regole	Descrizione	Data	
Elenco reputazione IP Amazon	`AWSManagedReconnaissanceList`	Aggiunta la `AWSManagedReconnaissanceList` regola in modalità monitoraggio/conteggio. Questa regola contiene gli indirizzi IP che eseguono la ricognizione delle risorse. AWS	2021-11-23

Sistema operativo Windows	`WindowsShellCommands`
	
	`PowerShellCommands`
		Sono state aggiunte tre nuove regole per WindowsShell i comandi:`WindowsShellCommands_COOKIE` , e. `WindowsShellCommands_QUERYARGUMENTS` `WindowsShellCommands_BODY`
		
		Aggiunta una nuova PowerShell regola:`PowerShellCommands_COOKIE` .
		
		Ha ristrutturato la denominaz
			2021-11-23

Gruppo di regole e regole	Descrizione	Data	
		ione `PowerShellComands` delle regole rimuovendo le stringhe _Set1 e _Set2. Sono state aggiunte firme di rilevamento più complete a. `PowerShellRules` È stata aggiunta la trasformazione `URL_DECODE_UNI` del testo a tutte le regole del sistema operativo Windows.	

Gruppo di regole e regole	Descrizione	Data	

Sistema operativo Linux	`LFI_URIPATH`
	
	`LFI_QUERYSTRING`
	
	`LFI_BODY`
	
	`LFI_COOKIE`
		La doppia trasforma zione del testo è stata sostituita con doppia`URL_DECODE` . `URL_DECODE_UNI`
		
		Aggiunta `NORMALIZE _PATH_WIN` come seconda trasforma zione del testo.
		
		Ha sostituito la `LFI_BODY` regola con la `LFI_COOKIE` regola.
		
		Sono state aggiunte firme di rilevamento più complete per tutte le `LFI` regole.
			2021-11-23

Core rule set (CRS)	`SizeRestr ictions_BODY`	Ridotto il limite di dimensione per bloccare le richieste Web con payload body superiori a 8 KB. In precedenza, il limite era di 10 KB.	2021-10-27

Gruppo di regole e regole	Descrizione	Data	

Core rule set (CRS)	`EC2MetaDataSSRF_BODY`
	`EC2MetaDataSSRF_COOKIE`
	`EC2MetaDataSSRF_URIPATH`
	`EC2MetaDataSSRF_QUERYARGUMENTS`
		Aggiunte altre firme di rilevamento. Aggiunta una doppia decodifica URL Unicode per migliorare il blocco.	27/10/2021

Core rule set (CRS)	`GenericLFI_QUERYARGUMENTS`
	`GenericLFI_URIPATH`
	`RestrictedExtensions_URIPATH`
	`RestrictedExtensions_QUERYARGUMENTS`
		Aggiunta una doppia decodifica URL Unicode per migliorare il blocco.	27/10/2021

Gruppo di regole e regole	Descrizione	Data	

Core rule set (CRS)	`GenericRFI_QUERYARGUMENTS`
	`GenericRFI_BODY`
	`GenericRFI_URIPATH`
		Sono state aggiornate le firme delle regole per ridurre i falsi positivi, in base al feedback dei clienti. È stata aggiunta una doppia decodifica URL Unicode per migliorare il blocco.	27/10/2021

Tutti	Tutte le regole	È stato aggiunto il supporto per le AWS WAF etichette a tutte le regole che non supportavano già l'etichettatura.	25-10-2021
Elenco reputazione IP Amazon	`AWSManagedIPReputationList_xxxx`	Ha ristrutturato l'elenco di reputazione IP, rimosso i suffissi dal nome della regola e aggiunto il supporto per le etichette. AWS WAF	04-05-2021
Elenco IP anonimi	`AnonymousIPList` `HostingProviderList`	Aggiunto il supporto per le etichette. AWS WAF	04-05-04
Controllo dei bot	Tutti	Aggiunto il set di regole Bot Control.	01/04/2021

Gruppo di regole e regole	Descrizione	Data	
Core rule set (CRS)	`GenericRFI_QUERYARGUMENTS`	Aggiunta doppia decodifica URL.	03/03/2021
Core rule set (CRS)	`RestrictedExtensions_URIPATH`	Migliorata la configurazione delle regole e aggiunta una decodifica URL aggiuntiva.	03/03/2021
Admin protection	`AdminProtection_URIPATH`	Aggiunta doppia decodifica URL.	03/03/2021
Known bad inputs	`ExploitablePaths_URIPATH`	Migliorata la configurazione delle regole e aggiunta una decodifica URL aggiuntiva.	03/03/2021
Sistema operativo Linux	`LFI_QUERYARGUMENTS`	Migliorata la configurazione delle regole e aggiunta una decodifica URL aggiuntiva.	03/03/2021
Sistema operativo Windows	Tutti	Migliorata la configurazione delle regole.	2020-09-23

Gruppo di regole e regole	Descrizione	Data	

Applicazione PHP	`PHPHighRiskMethodsVariables_QUERYARGUMENTS`
	
	`PHPHighRiskMethodsVariables_BODY`
		È stata modificata la trasformazione del testo dalla decodifica HTML alla decodifica URL, per migliorare il blocco.	16/09/2020

sistema operativo POSIX	`UNIXShellCommandsVariables_QUERYARGUMENTS`
	
	`UNIXShellCommandsVariables_BODY`
		È stata modificata la trasformazione del testo dalla decodifica HTML alla decodifica URL, per migliorare il blocco.	16/09/2020

Set di regole di base	`GenericLFI_QUERYARGUMENTS`
	
	`GenericLFI_URIPATH`
	
	GenericLFI_BODY
		È stata modificata la trasformazione del testo dalla decodifica HTML alla decodifica URL, per migliorare il blocco.	2020-08-07

Sistema operativo Linux	`LFI_URIPATH`
	
	`LFI_QUERYARGUMENTS`
	
	`LFI_BODY`
		Modificata la trasformazione del testo da decodifica a entità HTML a decodifica URL, per migliorare il rilevamento e il blocco.	2020-05-19

Gruppo di regole e regole	Descrizione	Data	
Elenco IP anonimo	Tutti	Nuovo gruppo di regole Gruppi di regole Reputazione IP per bloccare le richieste provenien ti da servizi che consentono di offuscare l'identità degli spettatori, per contribuire a mitigare i bot e l'elusione delle restrizioni geografic he.	06/03/2020
WordPress applicazi one	`WordPress Exploitab leCommand s_QUERYSTRING`	Nuova regola che controlla la presenza di comandi sfruttabili nella stringa di query.	03/03/2020

Core rule set (CRS)	`SizeRestr ictions_Q UERYSTRING`
	
	`SizeRestr ictions_C ookie_HEADER`
	
	`SizeRestr ictions_BODY`
	
	`SizeRestr ictions_U RIPATH`
		Regolazione dei vincoli del valore di dimensione per una maggiore precisione.	2020-03-03

Gruppo di regole e regole	Descrizione	Data	
Database SQL	`SQLi_URIPATH`	Le regole ora controllano l'URI del messaggio.	2020-01-23

Database SQL	`SQLi_BODY`
	
	`SQLi_QUERYARGUMENTS`
	
	`SQLi_COOKIE`
		Trasformazioni di testo aggiornate.	2019-12-20

Core rule set (CRS)	`CrossSite Scripting_URIPATH`
	
	`CrossSite Scripting_BODY`
	
	`CrossSite Scripting_QUERYARGUMENTS`
	
	`CrossSite Scripting_COOKIE`
		Trasformazioni di testo aggiornate.	2019-12-20

Marketplace AWS gruppi di regole gestiti

Marketplace AWS i gruppi di regole gestiti sono disponibili in abbonamento tramite la Marketplace AWS console all'indirizzo Marketplace AWS. Dopo esserti abbonato a un gruppo di regole Marketplace AWS gestito, puoi utilizzarlo in AWS WAF. Per utilizzare un gruppo di Marketplace AWS regole in una AWS Firewall Manager AWS WAF politica, ogni account dell'organizzazione deve sottoscriverlo.

Testa e ottimizza eventuali modifiche alle tue AWS WAF protezioni prima di utilizzarle per il traffico di produzione. Per informazioni, consulta Test e ottimizzazione delle protezioni AWS WAF.

Marketplace AWS Regole relative ai prezzi per gruppi

Marketplace AWS i gruppi di regole sono disponibili senza contratti a lungo termine e senza impegni minimi. Al momento della sottoscrizione a un gruppo di regole, vengono addebitate una tariffa mensile (ripartita proporzionalmente nell'ora), nonché le tariffe continue basate sul volume delle richieste. Per ulteriori informazioni, consulta la sezione AWS WAF Prezzi e la descrizione di ciascun gruppo di Marketplace AWS regole all'indirizzo Marketplace AWS.

Hai domande su un gruppo di Marketplace AWS regole?

Per domande su un gruppo di regole gestito da un Marketplace AWS venditore e per richiedere modifiche alle funzionalità, contatta il team di assistenza clienti del fornitore. Per trovare le informazioni di contatto, consulta l'elenco del fornitore all'indirizzo Marketplace AWS.

Il fornitore del gruppo di Marketplace AWS regole determina come gestire il gruppo di regole, ad esempio come aggiornare il gruppo di regole e se il gruppo di regole è dotato di versioni. Il provider determina inoltre i dettagli del gruppo di regole, incluse le regole, le azioni delle regole e le eventuali etichette che le regole aggiungono alle richieste Web corrispondenti.

Iscrizione a gruppi di regole Marketplace AWS gestiti

È possibile sottoscrivere e annullare l'iscrizione ai gruppi di Marketplace AWS regole sulla AWS WAF console.

> **Important**
>
> Per utilizzare un gruppo di Marketplace AWS regole in una AWS Firewall Manager politica, ogni account dell'organizzazione deve prima sottoscrivere quel gruppo di regole.

Per sottoscrivere un gruppo di regole Marketplace AWS gestito

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, scegli Marketplace AWS.
3. Nella sezione Available marketplace products (Prodotti Marketplace disponibili), scegliere il nome di un gruppo di regole per visualizzare dettagli e informazioni sui prezzi.

4. Se si desidera effettuare la sottoscrizione al gruppo di regole, scegliere Continue (Continua).

> **Note**
>
> Se non si desidera effettuare la sottoscrizione a questo gruppo di regole, è sufficiente chiudere questa pagina nel browser.

5. Scegliere Set up your account (Configura account).
6. Aggiungere il gruppo di regole a un'ACL Web, in modo simile all'aggiunta di una singola regola. Per ulteriori informazioni, consulta Creazione di un'ACL Web o Modifica di un ACL Web.

> **Note**
>
> Quando si aggiunge un gruppo di regole a un ACL Web, è possibile sovrascrivere le azioni delle regole nel gruppo di regole e del risultato del gruppo di regole. Per ulteriori informazioni, consulta Le azioni sostituiscono i gruppi di regole.

Dopo esserti iscritto a un gruppo di Marketplace AWS regole, lo usi negli ACL web come fai con altri gruppi di regole gestiti. Per informazioni, consulta Creazione di un'ACL Web.

Annullamento dell'iscrizione ai gruppi di regole gestiti Marketplace AWS

È possibile annullare l'iscrizione ai gruppi di Marketplace AWS regole sulla console. AWS WAF

> **Important**
>
> Per interrompere i costi di abbonamento per un gruppo di regole Marketplace AWS gestito, è necessario rimuoverlo da tutti gli ACL Web inclusi in AWS WAF e in qualsiasi AWS WAF politica di Firewall Manager, oltre a annullare l'iscrizione. Se annulli l'iscrizione a un gruppo di regole Marketplace AWS gestito ma non lo rimuovi dai tuoi ACL web, continuerai a ricevere i costi dell'abbonamento.

Per annullare l'iscrizione a un gruppo di regole gestito Marketplace AWS

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

2. Rimuovere il gruppo di regole da tutte le ACL Web. Per ulteriori informazioni, consulta Modifica di un ACL Web.
3. Nel riquadro di navigazione, scegli Marketplace AWS.
4. Scegliere Manage your subscriptions (Gestisci sottoscrizioni).
5. Scegliere Cancel subscription (Annulla sottoscrizione) accanto al nome del gruppo di regole di cui si desidera annullare la sottoscrizione.
6. Scegliere Yes, cancel subscription (Sì, annulla sottoscrizione).

Risoluzione dei problemi dei gruppi di Marketplace AWS regole

Se scopri che un gruppo di Marketplace AWS regole sta bloccando il traffico legittimo, puoi risolvere il problema eseguendo le seguenti operazioni.

Per risolvere i problemi relativi a un gruppo di regole Marketplace AWS

1. Sostituisci le azioni per conteggiare le regole che bloccano il traffico legittimo. Puoi identificare quali regole bloccano richieste specifiche utilizzando le richieste o i AWS WAF log campionati. AWS WAF Puoi identificare le regole osservando il campo `ruleGroupId` nel log o il `RuleWithinRuleGroup` nella richiesta campionata. È possibile identificare la regola nel modello. `<Seller Name>#<RuleGroup Name>#<Rule Name>`
2. Se l'impostazione di regole specifiche per contare solo le richieste non risolve il problema, puoi sovrascrivere tutte le azioni della regola o modificare l'azione per il gruppo di Marketplace AWS regole stesso da Nessuna sovrascrittura a Sostituisci per contare. Ciò consente il transito della richiesta Web, indipendentemente dalle singole operazioni delle regole all'interno del gruppo di regole.
3. Dopo aver ignorato l'azione della singola regola o dell'intero gruppo di Marketplace AWS regole, contatta il team di assistenza clienti del fornitore del gruppo di regole per risolvere ulteriormente il problema. Per informazioni di contatto, consulta l'elenco dei gruppi di regole nelle pagine di elenco dei prodotti su Marketplace AWS.

Contattare l'assistenza AWS

Per problemi AWS WAF o relativi a un gruppo di regole gestito da AWS, contatta AWS Support.
Per problemi con un gruppo di regole gestito da un Marketplace AWS venditore, contatta il team di assistenza clienti del provider. Per trovare le informazioni di contatto, consulta l'elenco del fornitore su Marketplace AWS.

Gestione dei propri gruppi di regole

Puoi creare il tuo gruppo di regole per riutilizzare le raccolte di regole che non trovi nelle offerte dei gruppi di regole gestite o che preferisci gestire autonomamente.

I gruppi di regole creati mantengono regole allo stesso modo di un'ACL Web ed è possibile aggiungere regole a un gruppo di regole allo stesso modo di un'ACL Web. Quando crei un tuo gruppo di regole, devi impostare una capacità massima non modificabile per lo stesso.

Argomenti

Creazione di un gruppo di regole

Per creare un gruppo di regole

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, scegliere Rule groups (Gruppi di regole), quindi Create rule group (Crea gruppo di regole).
3. Immettere un nome e una descrizione per il gruppo di regole. Li utilizzerai per identificare il set di regole per gestirlo e utilizzarlo.

   Non utilizzare nomi che iniziano con `AWSShield`,`PreFM`, o`PostFM`. Queste stringhe sono riservate o potrebbero creare confusione con i gruppi di regole gestiti dall'utente da altri servizi. Per informazioni, consulta Gruppi di regole forniti da altri servizi.

   > **Note**
   >
   > Non è possibile modificare il nome dopo aver creato il gruppo di regole.

4. Per Region (Regione), scegliere la regione in cui si desidera archiviare il gruppo di regole. Per utilizzare un gruppo di regole negli ACL Web che proteggono CloudFront le distribuzioni

Amazon, devi utilizzare l'impostazione globale. È possibile utilizzare l'impostazione globale anche per le applicazioni regionali.

5. Seleziona Successivo.
6. Aggiungere regole al gruppo di regole utilizzando la procedura guidata Rule builder (Generatore di regole), in modo analogo a come si fa nella gestione dell'ACL Web. La sola differenza è che non è possibile aggiungere un gruppo di regole a un altro gruppo di regole.
7. Per Capacity (Capacità), impostare l'utilizzo massimo delle unità di capacità ACL Web (WCU) per il gruppo di regole. Questa è un'impostazione non modificabile. Per informazioni sulle WCU, consulta AWS WAF unità di capacità Web ACL (WCU).

   Quando si aggiungono regole al gruppo di regole, nel riquadro Add rules and set capacity (Aggiungi regole e imposta capacità) viene visualizzata la capacità minima richiesta, basata sulle regole già aggiunte. È possibile utilizzare questo e i piani futuri per il gruppo di regole per stimare la capacità richiesta dal gruppo di regole.
8. Rivedere le impostazioni per il gruppo di regole e scegliere Create (Crea).

Modifica di un gruppo di regole

Per aggiungere o rimuovere regole da un gruppo di regole o modificare le impostazioni di configurazione, accedi al gruppo di regole utilizzando la procedura riportata in questa pagina.

> ⚠ Rischio legato al traffico di produzione
>
> Se modifichi un gruppo di regole che stai attualmente utilizzando in un ACL Web, tali modifiche influiranno sul comportamento dell'ACL Web ovunque venga utilizzato. Assicurati di testare e ottimizzare tutte le modifiche in un ambiente di staging o di test finché non ti senti a tuo agio con il potenziale impatto sul tuo traffico. Quindi testa e ottimizza le regole aggiornate in modalità di conteggio con il traffico di produzione prima di attivarle. Per le linee guida, consulta Test e ottimizzazione delle protezioni AWS WAF.

Per modificare un gruppo di regole

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, scegliere Rule groups (Gruppi di regole).

3. Scegli il nome del gruppo di regole che desideri modificare. La console ti porta alla pagina del gruppo di regole.
4. Modifica il gruppo di regole in base alle esigenze. Puoi modificare le proprietà mutabili del gruppo di regole, in modo analogo a come hai fatto durante la creazione. La console salva le modifiche man mano che procedi.

> **Note**
>
> Se modifichi il nome di una regola e desideri che il nome della metrica della regola rifletta la modifica, devi aggiornare anche il nome della metrica. AWS WAF non aggiorna automaticamente il nome della metrica di una regola quando si modifica il nome della regola. Puoi cambiare il nome della metrica quando modifichi la regola nella console, utilizzando l'editor JSON delle regole. Puoi anche modificare entrambi i nomi tramite le API e in qualsiasi elenco JSON che utilizzi per definire l'ACL web o il gruppo di regole.

Incoerenze temporanee durante gli aggiornamenti

Quando si crea o si modifica un ACL Web o altre AWS WAF risorse, le modifiche richiedono poco tempo per essere propagate in tutte le aree in cui sono archiviate le risorse. Il tempo di propagazione può variare da pochi secondi a diversi minuti.

Di seguito sono riportati alcuni esempi delle incongruenze temporanee che potreste notare durante la propagazione delle modifiche:

- Dopo aver creato un ACL Web, se si tenta di associarlo a una risorsa, è possibile che venga visualizzata un'eccezione che indica che l'ACL Web non è disponibile.
- Dopo aver aggiunto un gruppo di regole a un ACL Web, le nuove regole del gruppo di regole potrebbero essere in vigore in un'area in cui viene utilizzato l'ACL Web e non in un'altra.
- Dopo aver modificato l'impostazione di un'azione della regola, è possibile vedere la vecchia azione in alcuni punti e la nuova azione in altri.
- Dopo aver aggiunto un indirizzo IP a un set IP utilizzato in una regola di blocco, il nuovo indirizzo potrebbe essere bloccato in un'area mentre è ancora consentito in un'altra.

Utilizzo del gruppo di regole in un ACL Web

Per utilizzare un gruppo di regole in un ACL Web, è necessario aggiungerlo all'ACL Web in una dichiarazione di riferimento del gruppo di regole.

Rischio legato al traffico di produzione

Prima di implementare modifiche all'ACL Web per il traffico di produzione, testale e ottimizzale in un ambiente di staging o di test finché non ti senti a tuo agio con il potenziale impatto sul traffico. Quindi testa e ottimizza le regole aggiornate in modalità di conteggio con il traffico di produzione prima di abilitarle. Per le linee guida, consulta Test e ottimizzazione delle protezioni AWS WAF.

Note

L'utilizzo di più di 1.500 WCU in un ACL Web comporta costi superiori al prezzo base dell'ACL Web. Per ulteriori informazioni, consulta AWS WAF unità di capacità Web ACL (WCU) e Prezzi di AWS WAF.

Sulla console, quando aggiungi o aggiorni le regole nel tuo ACL web, nella pagina Aggiungi regole e gruppi di regole, scegli Aggiungi regole, quindi scegli Aggiungi regole e gruppi di regole personali. Quindi, scegli Rule group (Gruppo di regole) e seleziona il gruppo di regole dall'elenco.

Nell'ACL Web, puoi modificare il comportamento di un gruppo di regole e le relative regole impostando le singole azioni delle regole Count o qualsiasi altra azione. Questo può aiutarti a fare cose come testare un gruppo di regole, identificare i falsi positivi dalle regole di un gruppo di regole e personalizzare il modo in cui un gruppo di regole gestito gestisce le tue richieste. Per ulteriori informazioni, consulta Le azioni sostituiscono i gruppi di regole.

Se il gruppo di regole contiene un'istruzione basata sulla tariffa, ogni ACL Web in cui si utilizza il gruppo di regole dispone di un monitoraggio e una gestione delle tariffe separati per la regola basata sulla tariffa, indipendentemente da qualsiasi altro ACL Web in cui si utilizza il gruppo di regole. Per ulteriori informazioni, consulta Istruzione regola basata sulla frequenza.

Incoerenze temporanee durante gli aggiornamenti

Quando si crea o si modifica un ACL Web o altre AWS WAF risorse, le modifiche richiedono poco tempo per essere propagate in tutte le aree in cui sono archiviate le risorse. Il tempo di propagazione può variare da pochi secondi a diversi minuti.

Di seguito sono riportati alcuni esempi delle incongruenze temporanee che potreste notare durante la propagazione delle modifiche:

- Dopo aver creato un ACL Web, se si tenta di associarlo a una risorsa, è possibile che venga visualizzata un'eccezione che indica che l'ACL Web non è disponibile.
- Dopo aver aggiunto un gruppo di regole a un ACL Web, le nuove regole del gruppo di regole potrebbero essere in vigore in un'area in cui viene utilizzato l'ACL Web e non in un'altra.
- Dopo aver modificato l'impostazione di un'azione della regola, è possibile vedere la vecchia azione in alcuni punti e la nuova azione in altri.
- Dopo aver aggiunto un indirizzo IP a un set IP utilizzato in una regola di blocco, il nuovo indirizzo potrebbe essere bloccato in un'area mentre è ancora consentito in un'altra.

Condivisione di un gruppo di regole con un altro account

Puoi condividere un gruppo di regole di tua proprietà con un altro AWS account, per utilizzarlo da parte di quell'account. Puoi farlo solo tramite l' AWS WAF API. Per ulteriori informazioni, PutPermissionPolicyconsulta l' AWS WAF API Reference.

Eliminazione di un gruppo di regole

Segui le linee guida in questa sezione per eliminare un gruppo di regole.

Eliminazione di set e gruppi di regole referenziati

Quando si elimina un'entità che è possibile utilizzare in un ACL Web, ad esempio un set di IP, un set di pattern regex o un gruppo di regole, AWS WAF verifica se l'entità è attualmente utilizzata in un ACL Web. Se rileva che è in uso, AWS WAF ti avvisa. AWS WAF è quasi sempre in grado di determinare se un'entità è referenziata da un ACL web. Tuttavia, in rari casi, potrebbe non essere in grado di farlo. Se vuoi essere sicuro che al momento non stia utilizzando l'entità, controllala negli ACL web prima di eliminarla. Se l'entità è un set di riferimento, controlla anche che nessun gruppo di regole la stia utilizzando.

Per eliminare un gruppo di regole

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, scegliere Rule groups (Gruppi di regole).
3. Scegliere il gruppo di regole da eliminare, quindi selezionare Delete (Elimina).

Gruppi di regole forniti da altri servizi

Se tu o un amministratore della tua organizzazione utilizzate AWS Firewall Manager o AWS Shield Advanced gestite la protezione delle risorse utilizzando AWS WAF, potresti vedere delle istruzioni di riferimento sui gruppi di regole aggiunte agli ACL web del tuo account.

I nomi di questi gruppi di regole iniziano con le seguenti stringhe:

- **`ShieldMitigationRuleGroup`**— Questi gruppi di regole sono gestiti AWS Shield Advanced e utilizzati per fornire una mitigazione automatica degli attacchi DDoS a livello di applicazione alle risorse protette a livello di applicazione (livello 7).

  Quando abiliti la mitigazione automatica degli attacchi DDoS a livello di applicazione per una risorsa protetta, Shield Advanced aggiunge uno di questi gruppi di regole all'ACL Web associato alla risorsa. Shield Advanced assegna all'istruzione di riferimento del gruppo di regole un'impostazione di priorità di 10.000.000, in modo che venga eseguita dopo le regole configurate nell'ACL Web. Per ulteriori informazioni su questi gruppi di regole, vedere. Mitigazione DDoS automatica a livello di applicazione Shield Advanced

  > **Warning**
  >
  > Non provate a gestire manualmente questo gruppo di regole nell'ACL web. In particolare, non eliminate manualmente l'istruzione di riferimento del gruppo di `ShieldMitigationRuleGroup` regole dall'ACL web. Questa operazione potrebbe avere conseguenze indesiderate per tutte le risorse associate all'ACL web. Utilizza invece Shield Advanced per disabilitare la mitigazione automatica per le risorse associate all'ACL web. Shield Advanced rimuoverà automaticamente il gruppo di regole quando non è necessario per la mitigazione automatica.

- **`PREFMManaged`**e **`POSTFMManaged`** — Questi gruppi di regole sono gestiti da AWS Firewall Manager. Firewall Manager li fornisce all'interno degli ACL Web creati e gestiti da Firewall

Manager. I nomi degli ACL Web iniziano con. `FMManagedWebACLV2` Per informazioni su questi ACL Web e gruppi di regole, vedere. AWS WAF politiche

AWS WAF regole

Una AWS WAF regola definisce come ispezionare le richieste web HTTP (S) e l'azione da intraprendere su una richiesta quando soddisfa i criteri di ispezione. Le regole vengono definite solo nel contesto di un gruppo di regole o di un ACL Web.

Le regole non esistono di AWS WAF per sé. Non sono AWS risorse e non hanno Amazon Resource Names (ARN). Puoi accedere a una regola per nome nel gruppo di regole o nell'ACL Web in cui è definita. Puoi gestire le regole e copiarle su altri ACL Web utilizzando la visualizzazione JSON del gruppo di regole o dell'ACL web che contiene la regola. È inoltre possibile gestirle tramite il generatore di regole della AWS WAF console, disponibile per gli ACL Web e i gruppi di regole.

Nome regola

Ogni regola richiede un nome. Evita i nomi che iniziano con `AWS` e i nomi utilizzati per i gruppi di regole o le regole gestite per te da altri servizi. Per informazioni, consulta Gruppi di regole forniti da altri servizi.

> **Note**
>
> Se modifichi il nome di una regola e desideri che il nome della metrica della regola rifletta la modifica, devi aggiornare anche il nome della metrica. AWS WAF non aggiorna automaticamente il nome della metrica di una regola quando si modifica il nome della regola. Puoi cambiare il nome della metrica quando modifichi la regola nella console, utilizzando l'editor JSON delle regole. Puoi anche modificare entrambi i nomi tramite le API e in qualsiasi elenco JSON che utilizzi per definire l'ACL web o il gruppo di regole.

Dichiarazione della regola

Ogni regola richiede inoltre una dichiarazione che definisca il modo in cui la regola esamina le richieste Web. L'istruzione della regola può contenere altre istruzioni annidate a qualsiasi profondità, a seconda della regola e del tipo di istruzione. Alcune istruzioni di regole richiedono una serie di criteri. Ad esempio, è possibile specificare fino a 10.000 indirizzi IP o intervalli di indirizzi IP per una regola di corrispondenza del set IP.

È possibile definire regole che controllano criteri come i seguenti:

- Gli script che potrebbero essere dannosi. Alcuni malintenzionati incorporano script che possono sfruttare le vulnerabilità nelle applicazioni Web. Questa operazione è nota come Cross-site scripting (XSS).
- Gli indirizzi IP o gli intervalli di indirizzi di origine delle richieste.
- Il paese o la posizione geografica di origine delle richieste.
- Lunghezza di una parte specificata della richiesta, ad esempio la stringa di query.
- Il codice SQL che potrebbe essere dannoso. I malintenzionati provano a estrarre i dati dal tuo database incorporando codice SQL dannoso in una richiesta Web. Questa operazione è nota come SQL injection.
- Le stringhe presenti nella richiesta, ad esempio, i valori nell'intestazione `User-Agent` o le stringhe di testo visualizzate nella stringa di query. È inoltre possibile usare espressioni regolari (regex) per specificare queste stringhe.
- Etichette che le regole precedenti dell'ACL Web hanno aggiunto alla richiesta.

Oltre alle istruzioni con criteri di ispezione delle richieste Web, come quelle nell'elenco precedente, AWS WAF supporta istruzioni logiche per `AND` e `NOT` che `OR` vengono utilizzate per combinare le istruzioni in una regola.

Ad esempio, in base alle richieste recenti ricevute da un utente malintenzionato, potreste creare una regola con un'`AND`istruzione logica che combini le seguenti istruzioni annidate:

- Le richieste provengono da 192.0.2.44.
- Contengono il valore `BadBot` nell'intestazione `User-Agent`.
- Sembrano includere codice di tipo SQL nella stringa di query.

In questo caso, la richiesta web deve corrispondere a tutte le istruzioni per ottenere una corrispondenza per il livello superiore. `AND`

Argomenti

- Istruzione regola basata sulla frequenza
- Dichiarazioni sulle regole del gruppo di regole

Operazione delle regole

L'azione della regola indica AWS WAF cosa fare con una richiesta Web quando corrisponde ai criteri definiti nella regola. Facoltativamente, puoi aggiungere un comportamento personalizzato a ciascuna azione della regola.

> **Note**
>
> Le azioni delle regole possono essere terminative o non terminative. Un'azione di terminazione interrompe la valutazione ACL Web della richiesta e consente alla richiesta di continuare verso l'applicazione protetta oppure la blocca.

Di seguito sono riportate le opzioni dell'operazione delle regole:

- Allow— AWS WAF consente di inoltrare la richiesta alla AWS risorsa protetta per l'elaborazione e la risposta. Si tratta di un'azione terminativa. Nelle regole che definisci, puoi inserire intestazioni personalizzate nella richiesta prima di inoltrarla alla risorsa protetta.
- Block— AWS WAF blocca la richiesta. Si tratta di un'azione terminativa. Per impostazione predefinita, la AWS risorsa protetta risponde con un codice di `403 (Forbidden)` stato HTTP. Nelle regole che definisci, puoi personalizzare la risposta. Quando AWS WAF blocca una richiesta, le impostazioni dell'Blockazione determinano la risposta che la risorsa protetta invia al client.
- Count— AWS WAF conta la richiesta ma non determina se consentirla o bloccarla. Si tratta di un'azione non terminante. AWS WAF continua a elaborare le regole rimanenti nell'ACL Web. Nelle regole che definisci, puoi inserire intestazioni personalizzate nella richiesta e aggiungere etichette alle quali altre regole possono corrispondere.
- CAPTCHAe Challenge — AWS WAF utilizza i puzzle CAPTCHA e le sfide silenziose per verificare che la richiesta non provenga da un bot e AWS WAF utilizza i token per tenere traccia delle recenti risposte positive dei clienti.

> **Note**
>
> Ti vengono addebitati costi aggiuntivi quando utilizzi l'azione CAPTCHA o Challenge regola in una delle tue regole o come regola che sostituisce un'azione in un gruppo di regole. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

Queste azioni sulle regole possono terminare o non terminare, a seconda dello stato del token nella richiesta:

- Non terminazione per un token valido e non scaduto: se il token è valido e non è scaduto in base al CAPTCHA configurato o al tempo di immunità alla sfida, gestisce la richiesta in modo simile all'azione. AWS WAF Count AWS WAF continua a controllare la richiesta web in base alle regole rimanenti nell'ACL web. Analogamente alla Count configurazione, nelle regole da voi definite potete facoltativamente configurare queste azioni con intestazioni personalizzate da inserire nella richiesta e aggiungere etichette alle quali altre regole possono corrispondere.
- Terminazione con una richiesta bloccata per un token non valido o scaduto: se il token non è valido o il timestamp indicato è scaduto, AWS WAF interrompe l'ispezione della richiesta Web e blocca la richiesta, analogamente all'azione. Block AWS WAF quindi risponde al client con un codice di risposta personalizzato. InfattiCAPTCHA, se il contenuto della richiesta indica che il browser del client è in grado di gestirla, AWS WAF invia un puzzle CAPTCHA in formato JavaScript interstiziale, progettato per distinguere i client umani dai bot. Per l'Challengeazione, AWS WAF invia un messaggio JavaScript interstitial con una sfida silenziosa progettata per distinguere i browser normali dalle sessioni gestite dai bot.

Per ulteriori informazioni, consulta CAPTCHAe Challenge in AWS WAF.

Per informazioni sulla personalizzazione delle richieste e delle risposte, consulta. Richieste e risposte web personalizzate in AWS WAF

Per informazioni sull'aggiunta di etichette alle richieste corrispondenti, vedereAWS WAF etichette sulle richieste web.

Per informazioni su come interagiscono l'ACL web e le impostazioni delle regole, consultaValutazione delle regole ACL Web e dei gruppi di regole.

Nozioni di base sulla dichiarazione delle regole

Le istruzioni delle regole sono la parte di una regola che spiega AWS WAF come ispezionare una richiesta web. Quando AWS WAF trova i criteri di ispezione in una richiesta web, diciamo che la richiesta web corrisponde all'istruzione. Ogni istruzione regola specifica cosa cercare e come cercarlo, in base al tipo di istruzione.

Ogni regola AWS WAF ha un'unica istruzione di primo livello, che può contenere altre istruzioni. Le istruzioni regola possono essere molto semplici. Ad esempio, potresti avere un'istruzione che fornisce una serie di paesi di origine da esaminare le tue richieste web oppure potresti avere una dichiarazione di regola in un ACL web che fa semplicemente riferimento a un gruppo di regole. Le istruzioni regola possono però essere anche molto complesse. Ad esempio, è possibile avere un'istruzione che combina molte altre istruzioni con istruzioni AND OR logiche e. NOT

Nidificazione di istruzioni regola

AWS WAF supporta l'annidamento per molte istruzioni di regole, ma non per tutte. Ad esempio, non è possibile annidare un'istruzione di un gruppo di regole all'interno di un'altra istruzione. È necessario utilizzare il nesting per alcuni scenari, come le istruzioni scope-down e le istruzioni logiche. Gli elenchi delle istruzioni e i dettagli delle regole che seguono descrivono le funzionalità e i requisiti di annidamento per ogni categoria e regola.

L'editor visivo per le regole nella console supporta solo un livello di nidificazione per le istruzioni delle regole. Ad esempio, puoi nidificare molti tipi di istruzioni all'interno di una logica AND o di una OR regola, ma non puoi nidificarne un'altraAND, perché ciò richiede un secondo livello di nidificazione. OR Per implementare più livelli di nesting, fornisci la definizione della regola in JSON, tramite l'editor di regole JSON nella console o tramite le API.

Argomenti

- Componenti delle richieste Web
- Dichiarazioni delimitate
- Dichiarazioni che fanno riferimento a un set o a un gruppo di regole

Componenti delle richieste Web

Questa sezione descrive le impostazioni che è possibile specificare per le istruzioni delle regole che esaminano un componente della richiesta Web. Per informazioni sull'utilizzo, consulta le singole istruzioni delle regole all'indirizzoDichiarazioni sulle regole della partita.

Un sottoinsieme di questi componenti può essere utilizzato anche nelle regole basate sulla frequenza, come chiavi di aggregazione delle richieste personalizzate. Per informazioni, consulta Opzioni e chiavi di aggregazione.

Per le impostazioni del componente di richiesta, specificate il tipo di componente stesso e le eventuali opzioni aggiuntive scelte, a seconda del tipo di componente. Ad esempio, se scegliete un tipo di componente che contiene testo da ispezionare, potete specificare le trasformazioni di testo AWS WAF da applicare prima di valutare i criteri di ispezione.

> **Note**
>
> Salvo diversa indicazione, se una richiesta web non ha il componente di richiesta specificato nell'istruzione della regola, AWS WAF valuta la richiesta come non conforme ai criteri della regola.

Indice

Richiedi le opzioni dei componenti

Questa sezione descrive i componenti della richiesta Web che è possibile specificare per l'ispezione. Si specifica il componente di richiesta per le istruzioni Match Rule che cercano modelli all'interno della richiesta web. Questi tipi di istruzioni includono string match, regex match, size constraint e istruzioni di attacco SQL injection. Per informazioni su come utilizzare queste impostazioni dei componenti di richiesta, consulta le singole istruzioni delle regole all'indirizzo Dichiarazioni sulle regole della partita

Salvo diversa indicazione, se una richiesta web non ha il componente di richiesta specificato nell'istruzione della regola, AWS WAF valuta la richiesta come non corrispondente ai criteri della regola.

> **Note**
>
> Si specifica un singolo componente di richiesta per ogni istruzione regola che lo richiede. Per ispezionare più componenti di una richiesta, creare un'istruzione regola per ogni componente.

La documentazione della AWS WAF console e dell'API fornisce indicazioni per le impostazioni del componente di richiesta nelle seguenti posizioni:

- Generatore di regole sulla console: nelle impostazioni di Statement per un tipo di regola normale, scegli il componente che desideri esaminare nella finestra di dialogo Ispeziona in Richiedi componenti.
- Contenuto della dichiarazione API: `FieldToMatch`

Il resto di questa sezione descrive le opzioni relative alla parte della richiesta web da esaminare.

Argomenti

- Metodo HTTP
- Intestazione singola
- Tutte le intestazioni
- Ordine delle intestazioni
- Cookie
- Percorso URI

- Impronta digitale JA3
- Stringa di query
- Parametro di query singola
- Tutti i parametri di query
- Body
- Corpo JSON

Metodo HTTP

Ispeziona il metodo HTTP per la richiesta. Il metodo HTTP indica il tipo di operazione che la richiesta Web richiede alla risorsa protetta di eseguire, ad esempio `POST` o`GET`.

Intestazione singola

Ispeziona una singola intestazione denominata nella richiesta. Per questa opzione, si specifica il nome dell'intestazione, ad esempio o. `User-Agent` `Referer` La corrispondenza tra stringhe per il nome non fa distinzione tra maiuscole e minuscole.

Tutte le intestazioni

Ispeziona tutte le intestazioni della richiesta, inclusi i cookie. Puoi applicare un filtro per ispezionare un sottoinsieme di tutte le intestazioni. Per questa opzione, fornisci le seguenti specifiche:

- Match Patterns: il filtro da utilizzare per ottenere un sottoinsieme di intestazioni da ispezionare. AWS WAF cerca questi pattern nei tasti delle intestazioni.

  L'impostazione dei modelli di corrispondenza può essere una delle seguenti:
  - Tutti: abbina tutti i tasti. Valuta i criteri di controllo delle regole per tutte le intestazioni.
  - Intestazioni escluse: ispeziona solo le intestazioni le cui chiavi non corrispondono a nessuna delle stringhe specificate qui. La corrispondenza tra stringhe per una chiave non fa distinzione tra maiuscole e minuscole.
  - Intestazioni incluse: ispeziona solo le intestazioni che hanno una chiave che corrisponde a una delle stringhe specificate qui. La corrispondenza tra stringhe per una chiave non fa distinzione tra maiuscole e minuscole.
- Ambito di corrispondenza: le parti delle intestazioni che AWS WAF devono essere controllate in base ai criteri di ispezione delle regole. È possibile specificare Chiavi, Valori o Tutto per controllare sia le chiavi che i valori per verificare una corrispondenza.

Tutto non richiede che venga trovata una corrispondenza nelle chiavi e una corrispondenza nei valori. Richiede la ricerca di una corrispondenza nelle chiavi o nei valori o in entrambi. Per richiedere una corrispondenza nelle chiavi e nei valori, utilizzate un'ANDistruzione logica per combinare due regole di corrispondenza, una che ispeziona le chiavi e l'altra che ispeziona i valori.

- Gestione di dimensioni eccessive: come gestire AWS WAF le richieste con dati di intestazione più grandi di quelli ispezionabili. AWS WAF AWS WAF può ispezionare al massimo i primi 8 KB (8.192 byte) delle intestazioni delle richieste e al massimo le prime 200 intestazioni. Il contenuto è disponibile per l'ispezione AWS WAF fino al primo limite raggiunto. È possibile scegliere di continuare l'ispezione oppure di saltarla e contrassegnare la richiesta come conforme o non conforme alla regola. Per ulteriori informazioni sulla gestione di contenuti di grandi dimensioni, consulta. Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF

Ordine delle intestazioni

Ispeziona una stringa contenente l'elenco dei nomi delle intestazioni della richiesta, ordinati così come appaiono nella richiesta web che AWS WAF riceve per l'ispezione. AWS WAF genera la stringa e poi la utilizza come campo per abbinare il componente durante la sua ispezione. AWS WAF separa i nomi delle intestazioni nella stringa con due punti e senza spazi aggiunti, ad esempio. `host:user-agent:accept:authorization:referer`

Per questa opzione, fornite le seguenti specifiche:

- Gestione sovradimensionata: come AWS WAF gestire le richieste con dati di intestazione più numerosi o più grandi di quelli che è AWS WAF possibile esaminare. AWS WAF può ispezionare al massimo i primi 8 KB (8.192 byte) delle intestazioni delle richieste e al massimo le prime 200 intestazioni. Il contenuto è disponibile per l'ispezione AWS WAF fino al primo limite raggiunto. Puoi scegliere di continuare a controllare le intestazioni disponibili oppure di saltare l'ispezione e contrassegnare la richiesta come corrispondente o non corrispondente alla regola. Per ulteriori informazioni sulla gestione di contenuti di grandi dimensioni, consulta. Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF

Cookie

Ispeziona tutti i cookie della richiesta. Puoi applicare un filtro per ispezionare un sottoinsieme di tutti i cookie. Per questa opzione, fornisci le seguenti specifiche:

- Match patterns: il filtro da utilizzare per ottenere un sottoinsieme di cookie da ispezionare. AWS WAF cerca questi modelli nelle chiavi dei cookie.

  L'impostazione dei modelli di corrispondenza può essere una delle seguenti:

  - Tutti: abbina tutti i tasti. Valuta i criteri di controllo delle regole per tutti i cookie.
  - Cookie esclusi: ispeziona solo i cookie le cui chiavi non corrispondono a nessuna delle stringhe specificate qui. La corrispondenza tra stringhe per una chiave fa distinzione tra maiuscole e minuscole e deve essere esatta.
  - Cookie inclusi: ispeziona solo i cookie che hanno una chiave che corrisponde a una delle stringhe specificate qui. La corrispondenza tra stringhe per una chiave fa distinzione tra maiuscole e minuscole e deve essere esatta.
- Match scope: le parti dei cookie che AWS WAF devono essere controllate in base ai criteri di ispezione delle regole. È possibile specificare Chiavi, Valori o Tutto sia per le chiavi che per i valori.

  Tutto non richiede che venga trovata una corrispondenza nelle chiavi e una corrispondenza nei valori. Richiede la ricerca di una corrispondenza nelle chiavi o nei valori o in entrambi. Per richiedere una corrispondenza nelle chiavi e nei valori, utilizzate un'`AND`istruzione logica per combinare due regole di corrispondenza, una che ispeziona le chiavi e l'altra che ispeziona i valori.
- Gestione sovradimensionata: come AWS WAF gestire le richieste che contengono dati dei cookie più AWS WAF grandi di quelli che è possibile ispezionare. AWS WAF può ispezionare al massimo i primi 8 KB (8.192 byte) dei cookie di richiesta e al massimo i primi 200 cookie. Il contenuto è disponibile per l'ispezione AWS WAF fino al primo limite raggiunto. È possibile scegliere di continuare l'ispezione oppure di saltarla e contrassegnare la richiesta come conforme o non conforme alla regola. Per ulteriori informazioni sulla gestione di contenuti di grandi dimensioni, consulta. Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF

Percorso URI

Controlla la parte di un URL che identifica una risorsa, ad esempio. `/images/daily-ad.jpg` Per informazioni, vedere Uniform Resource Identifier (URI): sintassi generica.

Se non utilizzate una trasformazione di testo con questa opzione, AWS WAF non normalizza l'URI e lo ispeziona esattamente come lo riceve dal client nella richiesta. Per informazioni sulle trasformazioni del testo, consulta. Trasformazioni di testo

Impronta digitale JA3

Controlla l'impronta digitale JA3 della richiesta. L'impronta digitale JA3 è un hash di 32 caratteri derivato dal TLS Client Hello di una richiesta in arrivo. Questa impronta digitale funge da identificatore univoco per la configurazione TLS del client. AWS WAF calcola e registra questa impronta digitale per ogni richiesta che contiene informazioni TLS Client Hello sufficienti per il calcolo. Quasi tutte le richieste web includono queste informazioni.

Come ottenere l'impronta digitale JA3 per un client

È possibile ottenere l'impronta digitale JA3 per le richieste di un client dai registri ACL Web. Se AWS WAF è in grado di calcolare l'impronta digitale, la include nei registri. Per informazioni sui campi di registrazione, vedere. Campi di log

Requisiti della dichiarazione delle regole

È possibile controllare l'impronta digitale JA3 solo all'interno di un'istruzione di corrispondenza delle stringhe impostata in modo che corrisponda esattamente alla stringa fornita. Fornisci la stringa di impronte digitali JA3 dai log nella specifica dell'istruzione String Match, in modo che corrisponda a eventuali richieste future con la stessa configurazione TLS. Per informazioni sull'istruzione string match, vedere. Istruzione regola di corrispondenza stringa

È necessario fornire un comportamento di riserva per questa dichiarazione di regola. Il comportamento di fallback è lo stato della corrispondenza che si desidera AWS WAF assegnare alla richiesta web se non AWS WAF è possibile calcolare l'impronta digitale JA3. Se scegli di abbinare, AWS WAF considera la richiesta come corrispondente all'istruzione della regola e applica l'azione della regola alla richiesta. Se scegli di non corrispondere, AWS WAF considera la richiesta come se non corrispondesse alla dichiarazione della regola.

Per utilizzare questa opzione di corrispondenza, è necessario registrare il traffico ACL Web. Per informazioni, consulta Registrazione del traffico AWS WAF ACL Web.

Stringa di query

Controlla la parte dell'URL che appare dopo un ? carattere, se presente.

> **Note**
>
> Per le istruzioni match di cross-site scripting, si consiglia di scegliere Tutti i parametri di query anziché Query string. Scegliendo Tutti i parametri di query si aggiungono 10 WCU al costo base.

Parametro di query singola

Ispeziona un singolo parametro di query definito come parte della stringa di query. AWS WAF controlla il valore del parametro specificato.

Per questa opzione, si specifica anche un argomento Query. Ad esempio, se l'URL è`www.xyz.com?UserName=abc&SalesRegion=seattle`, è possibile specificare `UserName` o `SalesRegion` per l'argomento della query. La lunghezza massima per il nome dell'argomento è di 30 caratteri. Il nome non fa distinzione tra maiuscole e minuscole, quindi se lo si specifica`UserName`, AWS WAF corrisponde a tutte le varianti di`UserName`, incluso `username` e`UsERName`.

Se la stringa di query contiene più di un'istanza dell'argomento di interrogazione specificato, AWS WAF controlla tutti i valori per individuare una corrispondenza, utilizzando la OR logica. Ad esempio, nell'URL `www.xyz.com?SalesRegion=boston&SalesRegion=seattle`, AWS WAF valuta il nome specificato rispetto a `boston` e `seattle`. Se uno dei due è una corrispondenza, l'ispezione è una corrispondenza.

Tutti i parametri di query

Ispeziona tutti i parametri di interrogazione nella richiesta. È simile alla scelta del componente del singolo parametro di query, ma AWS WAF controlla i valori di tutti gli argomenti all'interno della stringa di query. Ad esempio, se l'URL è `www.xyz.com?UserName=abc&SalesRegion=seattle`, AWS WAF attiva una corrispondenza se il valore di `UserName` o `SalesRegion` corrisponde ai criteri di ispezione.

La scelta di questa opzione aggiunge 10 WCU al costo base.

Body

Ispeziona il corpo della richiesta, valutato come testo semplice. Puoi anche valutare il corpo come JSON utilizzando il JSON tipo di contenuto.

Il corpo della richiesta è la parte della richiesta che segue immediatamente le intestazioni della richiesta. Contiene tutti i dati aggiuntivi necessari per la richiesta Web, ad esempio i dati di un modulo.

- Nella console, lo selezioni sotto l'opzione Request Body, selezionando l'opzione Tipo di contenuto Testo normale.
- Nell'API, nelle `FieldToMatch` specifiche della regola, specifichi di `Body` ispezionare il corpo della richiesta come testo semplice.

Per Application Load Balancer and AWS AppSync, AWS WAF può ispezionare i primi 8 KB del corpo di una richiesta. Infatti CloudFront, API Gateway, Amazon Cognito, App Runner e Verified Access, per impostazione predefinita, AWS WAF possono ispezionare i primi 16 KB e puoi aumentare il limite fino a 64 KB nella tua configurazione ACL web. Per ulteriori informazioni, consulta Gestione dei limiti di dimensione delle ispezioni corporee.

È necessario specificare la gestione delle dimensioni eccessive per questo tipo di componente. La gestione delle dimensioni eccessive definisce il modo in cui vengono AWS WAF gestite le richieste con dati corporei più grandi di quelli che è AWS WAF possibile esaminare. È possibile scegliere di continuare l'ispezione o di saltare l'ispezione e contrassegnare la richiesta come conforme o non conforme alla regola. Per ulteriori informazioni sulla gestione di contenuti di grandi dimensioni, consulta. Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF

Puoi anche valutare il corpo come JSON analizzato. Per informazioni a riguardo, consulta la sezione che segue.

Corpo JSON

Ispeziona il corpo della richiesta, valutato come JSON. Puoi anche valutare il corpo come testo semplice.

Il corpo della richiesta è la parte della richiesta che segue immediatamente le intestazioni della richiesta. Contiene tutti i dati aggiuntivi necessari per la richiesta Web, ad esempio i dati di un modulo.

- Nella console, lo selezioni sotto l'opzione Request Body, selezionando la scelta del tipo di contenuto JSON.
- Nell'API, nelle `FieldToMatch` specifiche della regola, si specifica`JsonBody`.

Per Application Load Balancer and AWS AppSync, AWS WAF può ispezionare i primi 8 KB del corpo di una richiesta. Infatti CloudFront, API Gateway, Amazon Cognito, App Runner e Verified Access, per impostazione predefinita, AWS WAF possono ispezionare i primi 16 KB e puoi aumentare il limite fino a 64 KB nella tua configurazione ACL web. Per ulteriori informazioni, consulta Gestione dei limiti di dimensione delle ispezioni corporee.

È necessario specificare la gestione delle dimensioni eccessive per questo tipo di componente. La gestione delle dimensioni eccessive definisce il modo in cui vengono AWS WAF gestite le richieste con dati corporei più grandi di quelli che è AWS WAF possibile esaminare. È possibile scegliere di continuare l'ispezione o di saltare l'ispezione e contrassegnare la richiesta come conforme o non conforme alla regola. Per ulteriori informazioni sulla gestione di contenuti di grandi dimensioni, consulta. Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF

Quando AWS WAF ispeziona il corpo della richiesta Web come JSON analizzato, analizza ed estrae gli elementi dal JSON e ispeziona le parti indicate utilizzando i criteri della dichiarazione di corrispondenza della regola.

La scelta di questa opzione raddoppia il costo base delle WCU del match statement. Ad esempio, se il costo base del match statement è di 5 WCU senza analisi JSON, l'utilizzo dell'analisi JSON raddoppia il costo portandolo a 10 WCU.

Con questa opzione, AWS WAF esegue due pattern di corrispondenza sul corpo della richiesta web. L'output del primo pattern di corrispondenza viene utilizzato come input per il secondo pattern di corrispondenza:

1. AWS WAF analizza ed estrae il contenuto JSON e identifica gli elementi da ispezionare. A tale scopo, AWS WAF utilizza i criteri forniti nella specifica del corpo JSON della regola.
2. AWS WAF applica qualsiasi trasformazione di testo agli elementi estratti e quindi abbina il set di elementi JSON risultante ai criteri di corrispondenza dell'istruzione della regola. Se uno qualsiasi degli elementi corrisponde, la richiesta web corrisponde alla regola.

Specificate i seguenti criteri AWS WAF da utilizzare per la prima fase di pattern matching, per identificare gli elementi JSON da ispezionare:

- Comportamento di riserva dell'analisi del corpo: cosa AWS WAF fare se non riesce ad analizzare completamente il corpo JSON. Le opzioni sono le seguenti:
  - Nessuno (comportamento predefinito): AWS WAF valuta il contenuto solo fino al punto in cui si è verificato un errore di analisi.

- Valuta come stringa: ispeziona il corpo come testo semplice. AWS WAF applica le trasformazioni del testo e i criteri di ispezione definiti per l'ispezione JSON alla stringa di testo del corpo.
- Match: considera la richiesta Web come se corrispondesse alla dichiarazione della regola. AWS WAF applica l'azione della regola alla richiesta.
- Nessuna corrispondenza: considera la richiesta Web come se non corrispondesse all'istruzione della regola.

AWS WAF fa del suo meglio per analizzare l'intero corpo JSON, ma potrebbe essere costretto a interrompersi per motivi quali caratteri non validi, chiavi duplicate, troncamento e qualsiasi contenuto il cui nodo principale non sia un oggetto o un array.

AWS WAF analizza il codice JSON negli esempi seguenti come due coppie chiave:valore valide:

- Virgola mancante: `{"key1":"value1""key2":"value2"}`
- Due punti mancanti: `{"key1":"value1","key2""value2"}`
- Colon in eccesso: `{"key1"::"value1","key2""value2"}`

- JSON match scope: i tipi di elementi del JSON che devono essere esaminati. AWS WAF È possibile specificare Chiavi, Valori o Tutto sia per le chiavi che per i valori.

  Tutto non richiede che venga trovata una corrispondenza nelle chiavi e una corrispondenza nei valori. Richiede la ricerca di una corrispondenza nelle chiavi o nei valori o in entrambi. Per richiedere una corrispondenza nelle chiavi e nei valori, utilizzate un'`AND`istruzione logica per combinare due regole di corrispondenza, una che ispeziona le chiavi e l'altra che ispeziona i valori.
- Contenuto da ispezionare: gli elementi del file JSON analizzato ed estratto che desideri ispezionare. AWS WAF

  È necessario specificare uno dei seguenti elementi:

  - Contenuto JSON completo: valuta tutti gli elementi nel file JSON analizzato.
  - Solo elementi inclusi: valuta solo gli elementi nel JSON che corrispondono ai criteri JSON Pointer forniti. Per informazioni sulla sintassi JSON Pointer, consultate la documentazione JavaScript di Internet Engineering Task Force (IETF) Object Notation (JSON) Pointer.

    Non utilizzare questa opzione per includere tutti i percorsi nel file JSON. Utilizza invece il contenuto JSON completo.

    Ad esempio, nella console, puoi fornire quanto segue:

    ```
    /dogs/0/name
    ```

```
/dogs/1/name
```

Nell'API o nella CLI, puoi fornire quanto segue:

```
"IncludedPaths": ["/dogs/0/name", "/dogs/1/name"]
```

Esempio di scenario di ispezione del corpo in formato JSON

Se l'impostazione degli elementi inclusi è`/a/b`, allora per il seguente corpo JSON:

```
{
  "a":{
    "c":"d",
    "b":{
      "e":{
        "f":"g"
      }
    }
  }
}
```

L'elenco seguente descrive cosa AWS WAF valuterebbe per ogni impostazione del match scope. La chiaveb, che fa parte del percorso degli elementi inclusi, non viene valutata.

- Per un ambito di corrispondenza impostato su all:`e`, `f`, `e`g.
- Per un match scope impostato su keys: `e` and`f`.
- Per un ambito di corrispondenza impostato su valori:`g`.

Indirizzo IP inoltrato

Questa sezione si applica alle istruzioni delle regole che utilizzano l'indirizzo IP di una richiesta Web. Per impostazione predefinita, AWS WAF utilizza l'indirizzo IP dall'origine della richiesta Web. Tuttavia, se una richiesta Web passa attraverso uno o più proxy o sistemi di bilanciamento del carico, l'origine della richiesta Web conterrà l'indirizzo dell'ultimo proxy e non l'indirizzo di origine del client. In questo caso, l'indirizzo del client di origine viene in genere inoltrato in un'altra intestazione HTTP. Questa intestazione è in genere `X-Forwarded-For` (XFF), ma può essere diversa.

Dichiarazioni di regole che utilizzano indirizzi IP

Le istruzioni delle regole che utilizzano gli indirizzi IP sono le seguenti:

- Corrispondenza set di IP- Controlla che l'indirizzo IP corrisponda agli indirizzi definiti in un set IP.
- Corrispondenza geografica- Utilizza l'indirizzo IP per determinare il paese e la regione di origine e confronta il paese di origine con un elenco di paesi.
- Istruzione regola basata sulla frequenza- Può aggregare le richieste in base ai propri indirizzi IP per garantire che nessun indirizzo IP individuale invii richieste a una velocità troppo elevata. È possibile utilizzare l'aggregazione degli indirizzi IP da sola o in combinazione con altre chiavi di aggregazione.

Puoi indicare di AWS WAF utilizzare un indirizzo IP inoltrato per ognuna di queste istruzioni di regole, dall'`X-Forwarded-For`intestazione o da un'altra intestazione HTTP, invece di utilizzare l'origine della richiesta web. Per i dettagli su come fornire le specifiche, consulta la guida per i singoli tipi di istruzioni delle regole.

> **Note**
>
> Se l'intestazione specificata non è presente nella richiesta, AWS WAF significa che non applica affatto la regola alla richiesta web.

Comportamento di fallback

Quando si utilizza l'indirizzo IP inoltrato, si indica lo stato di corrispondenza AWS WAF da assegnare alla richiesta web se la richiesta non ha un indirizzo IP valido nella posizione specificata:

- MATCH: considera la richiesta web come se corrispondesse alla dichiarazione della regola. AWS WAF applica l'azione della regola alla richiesta.
- NESSUNA CORRISPONDENZA: considera la richiesta web come se non corrispondesse alla dichiarazione della regola.

Indirizzi IP utilizzati in AWS WAF Bot Control

Il gruppo di regole gestito da Bot Control verifica i bot utilizzando gli indirizzi IP di. AWS WAF Se utilizzi Bot Control e hai verificato i bot che effettuano il routing attraverso un proxy o un sistema di bilanciamento del carico, devi consentirli esplicitamente utilizzando una regola personalizzata. Ad esempio, puoi configurare una regola di corrispondenza del set di indirizzi IP personalizzata che

utilizza gli indirizzi IP inoltrati per rilevare e consentire i bot verificati. Puoi utilizzare la regola per personalizzare la gestione dei bot in diversi modi. Per maggiori informazioni ed esempi, consulta AWS WAF Controllo dei bot.

Considerazioni generali sull'utilizzo degli indirizzi IP inoltrati

Prima di utilizzare un indirizzo IP inoltrato, tieni presente le seguenti avvertenze generali:

- Un'intestazione può essere modificata dai proxy lungo il percorso e i proxy potrebbero gestire l'intestazione in modi diversi.
- Gli aggressori potrebbero alterare il contenuto dell'intestazione nel tentativo di aggirare le ispezioni. AWS WAF
- L'indirizzo IP all'interno dell'intestazione può essere malformato o non valido.
- L'intestazione specificata potrebbe non essere affatto presente in una richiesta.

Considerazioni sull'utilizzo degli indirizzi IP inoltrati con AWS WAF

L'elenco seguente descrive i requisiti e le avvertenze per l'utilizzo degli indirizzi IP inoltrati in: AWS WAF

- Per ogni singola regola, è possibile specificare un'intestazione per l'indirizzo IP inoltrato. La specifica dell'intestazione non fa distinzione tra maiuscole e minuscole.
- Per le istruzioni delle regole basate sulla frequenza, le istruzioni di scoping annidate non ereditano la configurazione IP inoltrata. Specificate la configurazione per ogni istruzione che utilizza un indirizzo IP inoltrato.
- Per le regole basate sulla corrispondenza geografica e sulla frequenza, AWS WAF utilizza il primo indirizzo nell'intestazione. Ad esempio, se un'intestazione contiene usi `10.1.1.1, 127.0.0.0, 10.10.10.10` AWS WAF `10.1.1.1`
- Per IP set match, si indica se corrispondere al primo, all'ultimo o a qualsiasi altro indirizzo nell'intestazione. Se ne specifichi una, AWS WAF controlla tutti gli indirizzi nell'intestazione per verificare se esiste una corrispondenza, fino a 10 indirizzi. Se l'intestazione contiene più di 10 indirizzi, AWS WAF controlla gli ultimi 10.
- Le intestazioni che contengono più indirizzi devono utilizzare un separatore di virgole tra gli indirizzi. Se una richiesta utilizza un separatore diverso dalla virgola, AWS WAF considera errati gli indirizzi IP nell'intestazione.

- Se gli indirizzi IP all'interno dell'intestazione non sono corretti o non sono validi, AWS WAF indica che la richiesta Web corrisponde o non corrisponde alla regola, in base al comportamento di fallback specificato nella configurazione IP inoltrata.
- Se l'intestazione specificata non è presente in una richiesta, AWS WAF non applica affatto la regola alla richiesta. Ciò significa che AWS WAF non applica l'azione della regola e non applica il comportamento di fallback.
- Una dichiarazione di regola che utilizza un'intestazione IP inoltrata per l'indirizzo IP non utilizzerà l'indirizzo IP riportato dall'origine della richiesta Web.

Le migliori pratiche per l'utilizzo di indirizzi IP inoltrati con AWS WAF

Quando utilizzi indirizzi IP inoltrati, utilizza le seguenti best practice:

- Valuta attentamente tutti i possibili stati delle intestazioni delle richieste prima di abilitare la configurazione IP inoltrata. Potrebbe essere necessario utilizzare più di una regola per ottenere il comportamento desiderato.
- Per ispezionare più intestazioni IP inoltrate o per ispezionare l'origine della richiesta Web e un'intestazione IP inoltrata, utilizzate una regola per ogni origine dell'indirizzo IP.
- Per bloccare le richieste Web con un'intestazione non valida, imposta l'azione della regola su block e imposta il comportamento di fallback per la configurazione IP inoltrata in modo che corrisponda.

Esempio JSON per indirizzi IP inoltrati

La seguente istruzione geo match corrisponde solo se l'`X-Forwarded-For`intestazione contiene un IP il cui paese di origine è: `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 seguente regola basata sulla frequenza aggrega le richieste in base al primo IP nell'intestazione. `X-Forwarded-For` La regola conta solo le richieste che corrispondono all'istruzione geo match annidata e blocca solo le richieste che corrispondono all'istruzione geo match. L'istruzione nested geo match utilizza anche l'`X-Forwarded-For`intestazione per determinare se l'indirizzo IP indica un paese di origine di. `US` In caso affermativo o se l'intestazione è presente ma non valida, l'istruzione geo match restituisce una corrispondenza.

```
{
  "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"
      }
    }
  }
}
```

Come ispezionare gli pseudo header HTTP/2

AWS Le risorse protette che supportano il traffico HTTP/2 non inoltrano le pseudo intestazioni HTTP/2 a fini di ispezione, ma forniscono il contenuto delle pseudo intestazioni nei AWS WAF componenti di richiesta Web che ispezionano. AWS WAF È possibile utilizzare AWS WAF per ispezionare solo le pseudo intestazioni elencate nella tabella seguente.

I contenuti delle pseudo intestazioni HTTP/2 sono mappati ai componenti della richiesta Web

Pseudo intestazione HTTP/2	Componente di richiesta Web da ispezionare	Documentazione
`:method`	Metodo HTTP	Metodo HTTP
`:authority`	`Host` Intestazione	Intestazione singola Tutte le intestazioni
`:path`Percorso URI	Percorso URI	Percorso URI
Query `:path`	Stringa di query	Stringa di query Parametro di query singola Tutti i parametri di query

Trasformazioni di testo

Nelle istruzioni che cercano modelli o impostano vincoli, potete fornire trasformazioni da applicare prima di AWS WAF esaminare la richiesta. Una trasformazione riformatta una richiesta Web per eliminare alcune formattazioni insolite utilizzate da utenti malintenzionati nel tentativo di escludere AWS WAF.

Quando lo usi con la selezione dei componenti della richiesta del corpo JSON, AWS WAF applica le trasformazioni dopo aver analizzato ed estratto gli elementi da ispezionare dal JSON. Per ulteriori informazioni, consulta Corpo JSON.

Se si forniscono più trasformazioni, si imposta anche l'ordine utilizzato da AWS WAF per applicarle.

WCU: ogni trasformazione di testo è composta da 10 WCU.

La documentazione della AWS WAF console e dell'API fornisce inoltre indicazioni per queste impostazioni nelle seguenti posizioni:

- Generatore di regole sulla console: trasformazione del testo. Questa opzione è disponibile quando utilizzi componenti di richiesta.
- Contenuto della dichiarazione API: `TextTransformations`

Opzioni per trasformazioni del testo

Ogni elenco di trasformazione mostra le specifiche della console e dell'API seguite dalla descrizione.

Base64 decode – `BASE64_DECODE`

AWS WAF decodifica una stringa con codifica Base64.

Base64 decode extension – `BASE64_DECODE_EXT`

AWS WAF decodifica una stringa con codifica Base64, ma utilizza un'implementazione indulgente che ignora i caratteri non validi.

Command line – `CMD_LINE`

Questa opzione mitiga le situazioni in cui gli aggressori potrebbero iniettare un comando dalla riga di comando del sistema operativo e utilizzare una formattazione insolita per mascherare alcuni o tutti i comandi.

Utilizza questa opzione per eseguire le seguenti trasformazioni:

- Eliminare i seguenti caratteri: `\ " ' ^`
- Eliminare gli spazi prima dei seguenti caratteri: `/ (`
- Sostituire i seguenti caratteri con uno spazio: `, ;`
- Sostituire più spazi con uno spazio
- Convertire lettere maiuscole, `A-Z`, in minuscole, `a-z`

Compress whitespace – `COMPRESS_WHITE_SPACE`

AWS WAF comprime lo spazio bianco sostituendo più spazi con uno spazio e sostituendo i seguenti caratteri con uno spazio (ASCII 32):

- Formfeed (ASCII 12)
- Scheda (ASCII 9)
- Nuova riga (ASCII 10)
- Carriage return (ASCII 13)
- Tabulazione verticale (ASCII 11)
- Spazio senza interruzioni (ASCII 160)

CSS decode – `CSS_DECODE`

AWS WAF decodifica i caratteri codificati utilizzando le regole di escape CSS 2.x. `syndata.html#characters` Questa funzione utilizza fino a due byte nel processo di decodifica, quindi può aiutare a scoprire caratteri ASCII che sono stati codificati usando la codifica CSS che in genere non verrebbe codificata. È utile anche per contrastare l'evasione, che è una combinazione di una barra rovesciata e caratteri non esadecimali. Ad esempio: `ja\vascript` per `javascript`.

Escape sequences decode – `ESCAPE_SEQ_DECODE`

AWS WAF decodifica le seguenti sequenze di escape ANSI C:`\a`,,,,,`\b`,`\f`,`\n`, `\r\t`, `\xHH` (esadecimale) `\v \\ \? \'\"`, (ottale). `\0000` Le codifiche non valide rimangono nell'output.

Hex decode – `HEX_DECODE`

AWS WAF decodifica una stringa di caratteri esadecimali in un binario.

HTML entity decode – `HTML_ENTITY_DECODE`

AWS WAF sostituisce i caratteri rappresentati in formato `&#xhhhh;` esadecimale o decimale con i caratteri corrispondenti. `&#nnnn;`

AWS WAF sostituisce i seguenti caratteri con codifica HTML con caratteri non codificati. Questo elenco utilizza la codifica HTML minuscola, ma la gestione non fa distinzione tra maiuscole e minuscole, ad esempio e viene trattata allo stesso modo. `&QuOt;` `"`

Carattere codificato in HTML	sostituito con...
`"`	"
`&`	&
`<`	<
`>`	>
` ` o ` `	spazio unificatore, decimale 160
`
`	\n, decimale 10
` `	\t, decimale 9
`{` o `{`	{
`|`, `|` o `|`	|
`}` o `}`	}
`!`	!
`#`	#
`$`	$
`&percent;` o `%`	%
`'`	\
`(`	(
`)`	)
`*` o `*`	*

Carattere codificato in HTML	sostituito con...
+	+
,	,
.	.
/	/
:	:
;	;
=	=
?	?
˜ o ˜	~
−	-
[o [	[
\	\\
] o]	]
&hat;	^
_ o &underbar;	_
` o `	`

JS decode – `JS_DECODE`

AWS WAF decodifica le sequenze di escape JavaScript . Se un `\uHHHH` codice rientra nell'intervallo di codici ASCII a larghezza intera di`FF01-FF5E`, viene utilizzato il byte superiore per rilevare e regolare il byte inferiore. In caso contrario, viene utilizzato solo il byte più basso e il byte più alto viene azzerato, causando una possibile perdita di informazioni.

Lowercase – `LOWERCASE`

AWS WAF converte le lettere maiuscole (A-Z) in minuscole (a-z).

MD5 – `MD5`

AWS WAF calcola un hash MD5 dai dati in input. L'hash calcolato è in una forma binaria grezza.

None – `NONE`

AWS WAF ispeziona la richiesta web così come è stata ricevuta, senza trasformazioni di testo.

Normalize path – `NORMALIZE_PATH`

AWS WAF normalizza la stringa di input rimuovendo più barre, riferimenti automatici alle directory e riferimenti retrospettivi alle directory che non si trovano all'inizio dell'input.

Normalize path Windows – `NORMALIZE_PATH_WIN`

AWS WAF converte i caratteri della barra rovesciata in barre in avanti e quindi elabora la stringa risultante utilizzando la trasformazione. `NORMALIZE_PATH`

Remove nulls – `REMOVE_NULLS`

AWS WAF rimuove tutti i `NULL` byte dall'input.

Replace comments – `REPLACE_COMMENTS`

AWS WAF sostituisce ogni occorrenza di un commento in stile C (/*... */) con un singolo spazio. Non comprime più occorrenze consecutive. Sostituisce i commenti non terminati con uno spazio (ASCII 0x20). Non modifica la terminazione autonoma di un commento (*/).

Replace nulls – `REPLACE_NULLS`

AWS WAF sostituisce ogni `NULL` byte dell'input con il carattere spazio (ASCII 0x20).

SQL hex decode – `SQL_HEX_DECODE`

AWS WAF decodifica i dati esadecimali SQL. Ad esempio, AWS WAF decodifica (`0x414243`) in (). `ABC`

URL decode – `URL_DECODE`

AWS WAF decodifica un valore con codifica URL.

URL decode Unicode – `URL_DECODE_UNI`

Tipo`URL_DECODE`, ma con supporto per la codifica specifica di Microsoft`%u`. Se il codice è nell'intervallo di codice ASCII a larghezza intera di `FF01-FF5E`, allora il byte più alto viene

utilizzato per rilevare e regolare il byte più basso. Altrimenti, viene utilizzato solo il byte più basso e il byte più alto viene azzerato.

UTF8 to Unicode – `UTF8_TO_UNICODE`

AWS WAF converte tutte le sequenze di caratteri UTF-8 in Unicode. Ciò aiuta a normalizzare l'input e a ridurre al minimo i falsi positivi e i falsi negativi per le lingue diverse dall'inglese.

Dichiarazioni delimitate

Un'istruzione scope-down è un'istruzione di regola nestable che si aggiunge all'interno di un'istruzione gestita di un gruppo di regole o di un'istruzione basata sulla frequenza per restringere il set di richieste valutate dalla regola contenente. La regola contenitore valuta solo le richieste che per prime corrispondono all'istruzione scope-down.

- Istruzione gestita del gruppo di regole: se aggiungi un'istruzione con ambito limitato a un'istruzione del gruppo di regole gestito, AWS WAF valuta qualsiasi richiesta che non corrisponde all'istruzione scope-down come non corrispondente al gruppo di regole. Solo le richieste che corrispondono all'istruzione scope-down vengono valutate rispetto al gruppo di regole. Per i gruppi di regole gestiti con prezzi basati sul numero di richieste valutate, le istruzioni dettagliate possono aiutare a contenere i costi.

  Per ulteriori informazioni sulle dichiarazioni dei gruppi di regole gestite, consulta. Istruzione gruppo di regole gestite
- Dichiarazione delle regole basata sulla frequenza: un'istruzione di regole basata sulla frequenza senza un'istruzione con ambito decrescente limita tutte le richieste valutate dalla regola. Se desideri controllare la frequenza solo per una categoria specifica di richieste, aggiungi un'istruzione con ambito limitato alla regola basata sulla frequenza. Ad esempio, per tenere traccia e controllare solo la frequenza delle richieste provenienti da un'area geografica specifica, puoi specificare quell'area geografica in un'istruzione di corrispondenza geografica e aggiungerla alla regola basata sulla tariffa come dichiarazione scope-down.

  Per ulteriori informazioni sulle istruzioni delle regole basate sulla tariffa, vedere. Istruzione regola basata sulla frequenza

È possibile utilizzare qualsiasi regola nestable in un'istruzione scope-down. Per le dichiarazioni disponibili, vedere e. Dichiarazioni sulle regole della partita Dichiarazioni di regole logiche Le WCU

per un'istruzione scope-down sono le WCU necessarie per l'istruzione della regola definita in essa. Non sono previsti costi aggiuntivi per l'utilizzo di un'istruzione scope-down.

È possibile configurare un'istruzione scope-down nello stesso modo in cui si utilizza l'istruzione in una regola normale. Ad esempio, puoi applicare trasformazioni di testo a un componente di richiesta Web che stai esaminando e puoi specificare un indirizzo IP inoltrato da utilizzare come indirizzo IP. Queste configurazioni si applicano solo all'istruzione scope-down e non vengono ereditate dal gruppo di regole gestito o dall'istruzione di regole basata sulla frequenza che lo contiene.

Ad esempio, se applicate trasformazioni di testo a una stringa di query nell'istruzione scope-down, l'istruzione scope-down controlla la stringa di query dopo aver applicato le trasformazioni. Se la richiesta soddisfa i criteri dell'istruzione scope-down, passa la richiesta Web alla regola contenitore nel suo stato originale AWS WAF , senza le trasformazioni dell'istruzione scope-down. La regola che contiene l'istruzione scope-down può applicare trasformazioni di testo proprie, ma non eredita alcuna dall'istruzione scope-down.

Non è possibile utilizzare un'istruzione scope-down per specificare alcuna configurazione di Request Inspection per l'istruzione della regola che la contiene. Non è possibile utilizzare un'istruzione scope-down come preprocessore di richieste Web per l'istruzione della regola che la contiene. L'unico ruolo di un'istruzione scope-down è determinare quali richieste vengono passate all'istruzione della regola che la contiene per l'ispezione.

Dichiarazioni che fanno riferimento a un set o a un gruppo di regole

Alcune regole utilizzano entità riutilizzabili e gestite al di fuori dei tuoi ACL Web, da te o da un Marketplace AWS venditore. AWS Quando l'entità riutilizzabile viene aggiornata, AWS WAF propaga l'aggiornamento alla regola. Ad esempio, se utilizzi un gruppo di regole AWS Managed Rules in un ACL web, quando AWS aggiorna il gruppo di regole, AWS propaga la modifica all'ACL web, per aggiornarne il comportamento. Se si utilizza un'istruzione IP set in una regola, quando si aggiorna il set, la modifica viene AWS WAF propagata a tutte le regole che vi fanno riferimento, in modo che tutti gli ACL Web che utilizzano tali regole vengano mantenuti con le modifiche apportate. up-to-date

Di seguito sono riportate le entità riutilizzabili che puoi utilizzare in un'istruzione regola.

- Set IP: puoi creare e gestire i tuoi set IP. Nella console, puoi accedere ad essi dal riquadro di navigazione. Per informazioni sulla gestione dei set di IP, consulta Set IP e set di pattern regex in AWS WAF.

- Set di partite regex: crei e gestisci i tuoi set di partite regex. Nella console, puoi accedere ad essi dal riquadro di navigazione. Per informazioni sulla gestione dei set del modello regex, consulta Set IP e set di pattern regex in AWS WAF.
- AWS Gruppi di regole gestite: AWS gestisce questi gruppi di regole. Nella console, sono disponibili per l'utilizzo quando aggiungi un gruppo di regole gestite all'ACL Web. Per ulteriori informazioni su queste impostazioni, consulta AWS Elenco dei gruppi di regole di Managed Rules.
- Marketplace AWS gruppi di regole gestiti: Marketplace AWS i venditori gestiscono questi gruppi di regole e puoi abbonarti per utilizzarli. Per gestire le sottoscrizioni, nel riquadro di navigazione della console, scegli Marketplace AWS. I gruppi di regole Marketplace AWS gestiti vengono elencati quando aggiungi un gruppo di regole gestito all'ACL web. Per i gruppi di regole a cui non sei ancora iscritto, puoi trovare anche un collegamento Marketplace AWS in quella pagina. Per maggiori informazioni sui gruppi di regole gestiti dai Marketplace AWS venditori, consultaMarketplace AWS gruppi di regole gestiti.
- I tuoi gruppi di regole: gestisci i tuoi gruppi di regole, di solito quando hai bisogno di un comportamento che non è disponibile tramite i gruppi di regole gestiti. Nella console, puoi accedere ad essi dal riquadro di navigazione. Per ulteriori informazioni, consulta Gestione dei propri gruppi di regole.

Eliminazione di un set di riferimento o gruppo di regole

Quando elimini un'entità referenziata, AWS WAF verifica se è attualmente utilizzata in un ACL web. Se AWS WAF rileva che è in uso, ti avvisa. AWS WAF è quasi sempre in grado di determinare se un'entità è referenziata da un ACL web. Tuttavia, in rari casi, potrebbe non essere in grado di farlo. Per assicurarti che l'entità che desideri eliminare non sia in uso, controlla nelle ACL Web prima di eliminarla.

Dichiarazioni sulle regole della partita

Le istruzioni Match confrontano la richiesta web o la sua origine con i criteri forniti dall'utente. Per molte istruzioni di questo tipo, AWS WAF confronta un componente specifico della richiesta per ottenere contenuti corrispondenti.

Le istruzioni Match sono instabili. È possibile annidare ognuna di queste istruzioni all'interno di istruzioni di regole logiche e utilizzarle in istruzioni scope-down. Per informazioni sulle istruzioni delle regole logiche, vedere. Dichiarazioni di regole logiche Per informazioni sulle istruzioni scope-down, vedere. Dichiarazioni delimitate

Questa tabella descrive le istruzioni di corrispondenza regolari che è possibile aggiungere a una regola e fornisce alcune linee guida per il calcolo dell'utilizzo delle unità di capacità Web ACL (WCU) per ciascuna di esse. Per informazioni sulle WCU, consulta AWS WAF unità di capacità Web ACL (WCU).

Istruzione di corrispondenza	Descrizione	WCU
Corrispondenza geografica	Controlla il paese di origine della richiesta e applica le etichette per il paese e la regione di origine.	1
Corrispondenza set di IP	Esamina la richiesta rispetto a una serie di indirizzi IP e intervalli di indirizzi.	1 per la maggior parte dei casi. Se configuri l'istruzione per utilizzare un'intestazione con indirizzi IP inoltrati e specifichi una posizione nell'intestazione diAny, aumenta le WCU di 4.
Dichiarazione della regola di corrispondenza delle etichette	Controlla la richiesta di etichette che sono state aggiunte da altre regole nello stesso ACL web.	1
Dichiarazione della regola Regex Match	Confronta un modello regex con un componente di richiesta specificato.	3, come costo base. Se si utilizza il componente di richiesta Tutti i parametri di interrogazione, aggiungere 10 WCU. Se utilizzi il corpo JSON del componente di richiesta, raddoppia il costo base delle WCU. Per ogni trasformazione di testo che applichi, aggiungi 10 WCU.

Istruzione di corrispondenza	Descrizione	WCU
Set del modello regex	Confronta i modelli di espressione regolare (regex) con un componente di richiesta specificato.	25 per set di pattern, come costo base. Se si utilizza il componente di richiesta Tutti i parametri di interrogazione, aggiungere 10 WCU. Se utilizzi il corpo JSON del componente di richiesta, raddoppia il costo base delle WCU. Per ogni trasformazione di testo che applichi, aggiungi 10 WCU.
Vincolo di dimensioni	Controlla i vincoli di dimension e rispetto a un componente di richiesta specificato.	1, come costo base. Se si utilizza il componente di richiesta Tutti i parametri di interrogazione, aggiungere 10 WCU. Se utilizzi il corpo JSON del componente di richiesta, raddoppia il costo base delle WCU. Per ogni trasformazione di testo che applichi, aggiungi 10 WCU.
Attacco SQLi	Controlla se è presente codice SQL dannoso in un componente di richiesta specificato.	20, come costo base. Se si utilizza il componente di richiesta Tutti i parametri di interrogazione, aggiungere 10 WCU. Se utilizzi il corpo JSON del componente di richiesta, raddoppia il costo base delle WCU. Per ogni trasformazione di testo che applichi, aggiungi 10 WCU.

Istruzione di corrispondenza	Descrizione	WCU
Corrispondenza stringa	Confronta una stringa con un componente di richiesta specificato.	Il costo base dipende dal tipo di corrispondenza tra stringhe ed è compreso tra 1 e 10. Se si utilizza il componente di richiesta Tutti i parametri di interrogazione, aggiungere 10 WCU. Se utilizzi il corpo JSON del componente di richiesta, raddoppia il costo base delle WCU. Per ogni trasformazione di testo che applichi, aggiungi 10 WCU.
Attacco XSS Scripting	Controlla se in un component e di richiesta specificato sono presenti attacchi cross-site scripting.	40, come costo base. Se si utilizza il componente di richiesta Tutti i parametri di interrogazione, aggiungere 10 WCU. Se utilizzi il corpo JSON del componente di richiesta, raddoppia il costo base delle WCU. Per ogni trasformazione di testo che applichi, aggiungi 10 WCU.

Istruzione regola di corrispondenza geografica

Utilizza le istruzioni geografiche o geo match per gestire le richieste web in base al paese e alla regione di origine. Un'istruzione geo match aggiunge etichette alle richieste web che indicano il paese di origine e la regione di origine. Aggiunge queste etichette indipendentemente dal fatto che i criteri della dichiarazione corrispondano alla richiesta. Un'istruzione geo match esegue anche la corrispondenza con il paese di origine della richiesta.

Come usare l'istruzione geo match

È possibile utilizzare l'istruzione geo match per la corrispondenza di paesi o regioni, come segue:

- Paese: puoi utilizzare una regola di geo match a sé stante per gestire le richieste in base esclusivamente al paese di origine. La dichiarazione delle regole corrisponde ai codici dei paesi. Puoi anche seguire una regola di corrispondenza geografica con una regola di corrispondenza delle etichette che corrisponde all'etichetta del paese di origine.
- Regione: utilizza una regola di corrispondenza geografica seguita da una regola di corrispondenza delle etichette per gestire le richieste in base alla regione di origine. Non puoi utilizzare una regola di corrispondenza geografica da sola per la corrispondenza con i codici regionali.

Per informazioni sull'utilizzo delle regole di abbinamento delle etichette, consulta Dichiarazione della regola di corrispondenza delle etichette eAWS WAF etichette sulle richieste web.

Come funziona l'istruzione geo match

Con l'istruzione geo match, AWS WAF gestisce ogni richiesta web come segue:

1. Determina i codici del paese e dell'area geografica della richiesta: AWS WAF determina il paese e la regione di una richiesta in base al relativo indirizzo IP. Per impostazione predefinita, AWS WAF utilizza l'indirizzo IP dell'origine della richiesta Web. È possibile indicare di AWS WAF utilizzare un indirizzo IP da un'intestazione di richiesta alternativa, ad esempio `X-Forwarded-For` abilitando la configurazione IP inoltrata nelle impostazioni della dichiarazione delle regole.

   AWS WAF determina la posizione delle richieste utilizzando i database MaxMind GeoIP. MaxMind riporta un'accuratezza molto elevata dei propri dati a livello nazionale, sebbene la precisione vari in base a fattori come il paese e il tipo di IP. Per ulteriori informazioni su MaxMind, consulta Geolocalizzazione MaxMind IP. Se ritieni che uno qualsiasi dei dati GeoIP sia errato, puoi inviare una richiesta di correzione a Maxmind all'indirizzo MaxMind Correct GeoIP2 Data.

   AWS WAF utilizza i codici alfa-2 per paese e regione dello standard 3166 dell'Organizzazione internazionale per la standardizzazione (ISO). È possibile trovare i codici nelle seguenti posizioni:

   - Sul sito web ISO, puoi cercare i codici dei paesi su ISO Online Browsing Platform (OBP).
   - Su Wikipedia, i codici dei paesi sono elencati in ISO 3166-2.

     I codici regionali di un paese sono elencati all'URL. `https://en.wikipedia.org/wiki/ISO_3166-2:`*`<ISO country code>`* Ad esempio, le regioni degli Stati Uniti sono conformi allo standard ISO 3166-2:US e per l'Ucraina sono conformi allo standard ISO 3166-2:UA.

2. Determina l'etichetta del paese e l'etichetta della regione da aggiungere alla richiesta: le etichette indicano se l'istruzione geo match utilizza l'IP di origine o una configurazione IP inoltrata.

   - IP di origine

     L'etichetta del paese è`awswaf:clientip:geo:country:<ISO country code>`. Esempio per gli Stati Uniti:`awswaf:clientip:geo:country:US`.

     L'etichetta della regione è`awswaf:clientip:geo:region:<ISO country code>-<ISO region code>`. Esempio per l'Oregon negli Stati Uniti:`awswaf:clientip:geo:region:US-OR`.

   - IP inoltrato

     L'etichetta del paese è. `awswaf:forwardedip:geo:country:<ISO country code>` Esempio per gli Stati Uniti:`awswaf:forwardedip:geo:country:US`.

     L'etichetta della regione è`awswaf:forwardedip:geo:region:<ISO country code>-<ISO region code>`. Esempio per l'Oregon negli Stati Uniti:`awswaf:forwardedip:geo:region:US-OR`.

   Se il codice del paese o della regione non è disponibile per l'indirizzo IP specificato di una richiesta, AWS WAF utilizza XX nelle etichette, al posto del valore. Ad esempio, la seguente etichetta è per un IP client il cui prefisso internazionale non è disponibile: `awswaf:clientip:geo:country:XX` e la seguente è per un IP inoltrato il cui paese sono gli Stati Uniti, ma il cui codice regionale non è disponibile:. `awswaf:forwardedip:geo:region:US-XX`

3. Valuta il codice del paese della richiesta in base ai criteri della regola

L'istruzione geo match aggiunge etichette di paesi e regioni a tutte le richieste che esamina, indipendentemente dal fatto che trovi o meno una corrispondenza.

> **Note**
>
> AWS WAF aggiunge qualsiasi etichetta alla fine della valutazione della richiesta web di una regola. Per questo motivo, qualsiasi corrispondenza di etichette utilizzata rispetto alle etichette di un'istruzione geo match deve essere definita in una regola separata dalla regola che contiene l'istruzione geo match.

Se desideri controllare solo i valori delle regioni, puoi scrivere una regola di corrispondenza geografica con Count azione e con una singola corrispondenza del codice del paese, seguita da una regola di corrispondenza delle etichette per le etichette delle regioni. È necessario fornire un codice del paese per la valutazione della regola di geo match, anche per questo approccio. Puoi ridurre la registrazione e contare le metriche specificando un paese che è molto improbabile che sia una fonte di traffico verso il tuo sito.

CloudFront distribuzioni e funzionalità di restrizione geografica CloudFront

Per CloudFront le distribuzioni, se utilizzi la funzionalità di restrizione CloudFront geografica, tieni presente che la funzionalità non inoltra le richieste bloccate a. AWS WAF Inoltra le richieste consentite a. AWS WAF Se desideri bloccare le richieste in base alla geografia e ad altri criteri che puoi specificare AWS WAF, usa l'istruzione AWS WAF geo match e non utilizzare la funzione di restrizione CloudFront geografica.

Caratteristiche dell'istruzione Geo Match

Nestable: puoi annidare questo tipo di istruzione.

WCU: 1 WCU.

Impostazioni: questa istruzione utilizza le seguenti impostazioni:

- Prefissi nazionali: una serie di prefissi nazionali da confrontare per una corrispondenza geografica. Questi devono essere codici di paese a due caratteri tratti dai codici ISO alfa-2 dei paesi dello standard internazionale ISO 3166, ad esempio,. `["US","CN"]`
- (Facoltativo) Configurazione IP inoltrata: per impostazione predefinita, AWS WAF utilizza l'indirizzo IP nell'origine della richiesta Web per determinare il paese di origine. In alternativa, puoi configurare la regola per utilizzare un IP inoltrato in un'intestazione HTTP come invece. `X-Forwarded-For` AWS WAF utilizza il primo indirizzo IP nell'intestazione. Con questa configurazione, si specifica anche un comportamento di fallback da applicare a una richiesta Web con un indirizzo IP non valido nell'intestazione. Il comportamento di fallback imposta il risultato corrispondente per la richiesta, in modo che corrisponda o non corrisponda. Per ulteriori informazioni, consulta Indirizzo IP inoltrato.

Dove trovare questa dichiarazione sulle regole

- Generatore di regole sulla console: per l'opzione Richiesta, scegli Proviene da un paese in.
- API — GeoMatchStatement

Esempi

Puoi utilizzare l'istruzione geo match per gestire le richieste provenienti da paesi o regioni specifici. Ad esempio, se desideri bloccare le richieste provenienti da determinati paesi, ma consentire comunque le richieste provenienti da uno specifico set di indirizzi IP in tali paesi, puoi creare una regola con l'azione impostata su Block e le seguenti istruzioni annidate, mostrate in pseudocodice:

- Dichiarazione AND
  - Istruzione di corrispondenza geografica che elenca i paesi che desideri bloccare
  - Dichiarazione NOT
    - Istruzione del set di IP che specifica gli indirizzi IP che desideri consentire

Oppure, se desideri bloccare alcune regioni in determinati paesi, ma consentire comunque le richieste da altre regioni di quei paesi, puoi prima definire una regola di geo match con l'azione impostata su. Count Quindi, definisci una regola di corrispondenza delle etichette che corrisponda alle etichette di corrispondenza geografica aggiunte e gestisca le richieste in base alle tue esigenze.

Il seguente pseudo codice descrive un esempio di questo approccio:

1. Dichiarazione Geo Match che elenca i paesi con regioni che desideri bloccare, ma con l'azione impostata su Count. Questa etichetta etichetta ogni richiesta web indipendentemente dallo stato della corrispondenza e fornisce anche le metriche di conteggio per i paesi di interesse.
2. ANDdichiarazione con azione di blocco
   - Dichiarazione Label Match che specifica le etichette per i paesi che desideri bloccare
   - Dichiarazione N0T
     - Dichiarazione Label Match che specifica le etichette delle regioni dei paesi di cui desideri consentire l'accesso

Il seguente elenco JSON mostra un'implementazione delle due regole descritte nello pseudocodice precedente. Queste regole bloccano tutto il traffico proveniente dagli Stati Uniti ad eccezione del traffico proveniente da Oregon e Washington. L'istruzione geo match aggiunge etichette di paesi e regioni a tutte le richieste che esamina. La regola label match segue la regola geo match, quindi può corrispondere alle etichette di paesi e regioni che la regola geo match ha appena aggiunto. L'istruzione geo match utilizza un indirizzo IP inoltrato, quindi l'etichetta matching specifica anche le etichette IP inoltrate.

```
{
   "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"
    }
}
```

Come altro esempio, puoi combinare la corrispondenza geografica con regole basate sulla tariffa per dare priorità alle risorse per gli utenti di un particolare paese o regione. Crei un'istruzione basata sulla tariffa diversa per ogni dichiarazione geo match o label match che utilizzi per differenziare i tuoi utenti. Imposta un limite di tariffa più alto per gli utenti nel paese o nella regione preferiti e imposta un limite di tariffa più basso per gli altri utenti.

Il seguente elenco JSON mostra una regola di geo match seguita da regole basate sulla tariffa che limitano la velocità di traffico proveniente dagli Stati Uniti. Le regole consentono al traffico proveniente dall'Oregon di arrivare a un tasso più elevato rispetto al traffico proveniente da qualsiasi altra parte del paese.

```
{
  "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"
  }
}
```

Istruzione regola di corrispondenza set di IP

L'istruzione IP set match controlla l'indirizzo IP di una richiesta Web rispetto a un insieme di indirizzi IP e intervalli di indirizzi. Utilizzare questa opzione per consentire o bloccare le richieste Web in base agli indirizzi IP da cui provengono le richieste. Per impostazione predefinita, AWS WAF utilizza l'indirizzo IP dell'origine della richiesta Web, ma è possibile configurare la regola in modo che utilizzi invece un'intestazione HTTP. `X-Forwarded-For`

AWS WAF supporta tutti gli intervalli CIDR IPv4 e IPv6 ad eccezione di. `/0` Per ulteriori informazioni sulla notazione CIDR, consulta la voce Classless Inter-Domain Routing su Wikipedia. Un set di IP può contenere fino a 10.000 indirizzi IP o intervalli di indirizzi IP da controllare.

> **Note**
>
> Ogni regola di corrispondenza set di IP fa riferimento a un set di IP, creato e mantenuto indipendentemente dalle regole. È possibile utilizzare un singolo set IP in più regole e, quando si aggiorna il set di riferimento, vengono aggiornate AWS WAF automaticamente tutte le regole che vi fanno riferimento.
> Per informazioni sulla creazione e la gestione di un set IP, vedereCreazione e gestione di un set di IP.

Quando aggiungi o aggiorni le regole nel gruppo di regole o nell'ACL Web, scegli l'opzione IP set (Set di IP) e seleziona il nome del set di IP da utilizzare.

Nestable: puoi annidare questo tipo di istruzione.

WCU: 1 WCU per la maggior parte. Se configuri l'istruzione per utilizzare gli indirizzi IP inoltrati e specifichi una posizione diANY, aumenta l'utilizzo della WCU di 4.

Questa istruzione utilizza le seguenti impostazioni:

- Specifiche del set IP: scegli il set IP che desideri utilizzare dall'elenco o creane uno nuovo.
- (Facoltativo) Configurazione IP inoltrata: un nome di intestazione IP inoltrato alternativo da utilizzare al posto dell'origine della richiesta. Specificate se corrispondere al primo, all'ultimo o a qualsiasi altro indirizzo nell'intestazione. È inoltre necessario specificare un comportamento di fallback da applicare a una richiesta Web con un indirizzo IP non valido nell'intestazione specificata. Il comportamento di fallback imposta il risultato corrispondente per la richiesta, in modo che corrisponda o non corrisponda. Per ulteriori informazioni, consulta Indirizzo IP inoltrato.

Dove trovare questa dichiarazione sulle regole

- Generatore di regole sulla console: per l'opzione Richiesta, scegli Origini da un indirizzo IP in.
- Aggiungi la mia pagina di regole e gruppi di regole sulla console: scegli l'opzione IP set.
- API — IP SetReferenceStatement

Dichiarazione della regola di corrispondenza delle etichette

L'istruzione label match controlla le etichette presenti sulla richiesta Web rispetto a una specifica di stringa. Le etichette disponibili per l'ispezione di una regola sono quelle che sono già state aggiunte alla richiesta Web da altre regole nella stessa valutazione dell'ACL Web.

Le etichette non persistono al di fuori della valutazione Web ACL, ma puoi accedere alle metriche delle etichette CloudWatch e visualizzare i riepiloghi delle informazioni sulle etichette per qualsiasi ACL Web nella console. AWS WAF Per ulteriori informazioni, consultare Metriche e dimensioni delle etichette e Monitoraggio e ottimizzazione. Puoi anche vedere le etichette nei log. Per informazioni, consulta Campi di log.

> **Note**
>
> Un'istruzione label match può visualizzare solo le etichette delle regole valutate in precedenza nell'ACL Web. Per informazioni su come AWS WAF valuta le regole e i gruppi di regole in un ACL Web, vedere. Ordine di elaborazione delle regole e dei gruppi di regole in un ACL Web

Per ulteriori informazioni sull'aggiunta e la corrispondenza delle etichette, vedere. AWS WAF etichette sulle richieste web

Nestable: puoi annidare questo tipo di istruzione.

WCU: 1 WCU

Questa istruzione utilizza le seguenti impostazioni:

- Ambito di corrispondenza: impostalo su Label in modo che corrisponda al nome dell'etichetta e, facoltativamente, ai namespace e al prefisso precedenti. Impostalo su Namespace in modo che corrisponda ad alcune o tutte le specifiche del namespace e, facoltativamente, al prefisso precedente.
- Chiave: la stringa con cui vuoi confrontare. Se specificate un ambito di corrispondenza dello spazio dei nomi, questo dovrebbe specificare solo gli spazi dei nomi e, facoltativamente, il prefisso, con i due punti finali. Se si specifica un ambito di corrispondenza dell'etichetta, questo deve includere il nome dell'etichetta e, facoltativamente, i namespace e il prefisso precedenti.

Per informazioni su queste impostazioni, consulta Corrispondenza a un'etichetta e Esempi di abbinamenti tra etichette.

Dove trovare questa dichiarazione sulla regola

- Generatore di regole sulla console: per l'opzione Request, scegli Ha etichetta.
- API: LabelMatchStatement

Dichiarazione della regola Regex Match

Un'istruzione regex match indica di AWS WAF abbinare un componente della richiesta a una singola espressione regolare (regex). Una richiesta web corrisponde all'istruzione se il componente della richiesta corrisponde all'espressione regolare specificata.

Questo tipo di istruzione è una buona alternativa alle Istruzione regola di corrispondenza del set del modello regex situazioni in cui si desidera combinare i criteri di corrispondenza utilizzando la logica matematica. Ad esempio, se desideri che un componente di richiesta corrisponda ad alcuni modelli regex e non corrisponda ad altri, puoi combinare le istruzioni regex match utilizzando and theANDdichiarazione delle regole. NOTdichiarazione delle regole

AWS WAF supporta la sintassi del pattern utilizzata dalla libreria `libpcre` PCRE con alcune eccezioni. La libreria è documentata in PCRE - Perl Compatible Regular Expressions. Per informazioni sul AWS WAF supporto, vedere. Corrispondenza dei modelli di espressioni regolari in AWS WAF

Nestable: puoi annidare questo tipo di istruzione.

WCU: 3 WCU, come costo base. Se si utilizza il componente di richiesta Tutti i parametri di interrogazione, aggiungere 10 WCU. Se utilizzi il corpo JSON del componente di richiesta, raddoppia il costo base delle WCU. Per ogni trasformazione di testo che applichi, aggiungi 10 WCU.

Questo tipo di istruzione funziona su un componente di richiesta Web e richiede le seguenti impostazioni del componente di richiesta:

- Componente di richiesta: la parte della richiesta Web per ispezionare, ad esempio, una stringa di query o il corpo.

> **Warning**
>
> Se ispezionate i componenti della richiesta Body, JSON body, Headers o Cookies, leggete le limitazioni relative alla quantità di contenuto AWS WAF che può essere ispezionata. Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF

Per informazioni sui componenti della richiesta Web, consulta. Componenti delle richieste Web

- Trasformazioni di testo opzionali: trasformazioni che si desidera AWS WAF eseguire sul componente della richiesta prima di esaminarlo. Ad esempio, potete trasformare in lettere minuscole o normalizzare lo spazio bianco. Se specificate più di una trasformazione, le AWS WAF elabora nell'ordine elencato. Per informazioni, consulta Trasformazioni di testo.

Dove trovare questa dichiarazione di regole

- Generatore di regole sulla console: per il tipo Match, scegli l'espressione regolare Matches.
- API: RegexMatchStatement

Istruzione regola di corrispondenza del set del modello regex

La corrispondenza del set del modello regex controlla la parte della richiesta Web specificata per i modelli di espressioni regolari specificati all'interno di un set del modello regex.

AWS WAF supporta la sintassi del pattern utilizzata dalla libreria `libpcre` PCRE con alcune eccezioni. La libreria è documentata in PCRE - Perl Compatible Regular Expressions. Per informazioni sul AWS WAF supporto, vedere. Corrispondenza dei modelli di espressioni regolari in AWS WAF

> **Note**
>
> Ogni regola di corrispondenza del set del modello regex fa riferimento a un set del modello regex, che viene creato e mantenuto indipendentemente dalle regole. È possibile utilizzare un singolo pattern regex impostato in più regole e, quando si aggiorna il set di riferimento, AWS WAF vengono aggiornate automaticamente tutte le regole che vi fanno riferimento.
> Per informazioni sulla creazione e la gestione di un set del modello regex, consulta Creazione e gestione di un set del modello regex.

Un'istruzione regex pattern set match indica di AWS WAF cercare uno qualsiasi dei modelli nel set all'interno del componente di richiesta scelto. Una richiesta Web corrisponderà all'istruzione regola del set del modello se il componente della richiesta corrisponde a uno qualsiasi dei modelli nel set.

Se desideri combinare le corrispondenze dei tuoi pattern regex usando la logica, ad esempio per abbinarle ad alcune espressioni regolari e non ad altre, prendi in considerazione l'utilizzo. Dichiarazione della regola Regex Match

Nestable: puoi annidare questo tipo di istruzione.

WCU: 25 WCU, come costo base. Se utilizzi il componente di richiesta Tutti i parametri di interrogazione, aggiungi 10 WCU. Se utilizzi il corpo JSON del componente di richiesta, raddoppia il costo base delle WCU. Per ogni trasformazione di testo che applichi, aggiungi 10 WCU.

Questo tipo di istruzione funziona su un componente di richiesta Web e richiede le seguenti impostazioni del componente di richiesta:

- Componente di richiesta: la parte della richiesta Web per ispezionare, ad esempio, una stringa di query o il corpo.

  > **Warning**
  >
  > Se ispezionate i componenti della richiesta Body, JSON body, Headers o Cookies, leggete le limitazioni relative alla quantità di contenuto AWS WAF che può essere ispezionata. Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF

  Per informazioni sui componenti della richiesta Web, consulta. Componenti delle richieste Web
- Trasformazioni di testo opzionali: trasformazioni che si desidera AWS WAF eseguire sul componente della richiesta prima di esaminarlo. Ad esempio, potete trasformare in lettere minuscole o normalizzare lo spazio bianco. Se specificate più di una trasformazione, le AWS WAF elabora nell'ordine elencato. Per informazioni, consulta Trasformazioni di testo.

Questa istruzione richiede le seguenti impostazioni:

- Specificazione del set di pattern Regex: scegli il set di pattern regex che desideri utilizzare dall'elenco o creane uno nuovo.

Dove trovare questa dichiarazione di regole

- Generatore di regole sulla console: per il tipo Match, scegli String match condition > Matches pattern dal set di espressioni regolari.
- API — RegexPatternSetReferenceStatement

Istruzione regola vincolo di dimensioni

Un'istruzione con vincolo di dimensione confronta il numero di byte in un componente di richiesta Web con un numero fornito dall'utente e corrisponde in base ai criteri di confronto. Il criterio di confronto è un operatore come maggiore di (>) o minore di (<). Ad esempio, è possibile eseguire la corrispondenza su richieste che contengono una stringa di query con una dimensione superiore a 100 byte.

> **Note**
>
> Questa istruzione controlla solo la dimensione del componente di richiesta web. Non ispeziona il contenuto del componente.

Se ispezionate il percorso URI, qualsiasi elemento / nel percorso conta come un carattere. Ad esempio, il percorso URI `/logo.jpg` è lungo nove caratteri.

Nestable: puoi annidare questo tipo di istruzione.

WCU: 1 WCU, come costo base. Se si utilizza il componente di richiesta Tutti i parametri di interrogazione, aggiungere 10 WCU. Se utilizzi il corpo JSON del componente di richiesta, raddoppia il costo base delle WCU. Per ogni trasformazione di testo che applichi, aggiungi 10 WCU.

Questo tipo di istruzione funziona su un componente di richiesta Web e richiede le seguenti impostazioni del componente di richiesta:

- Componente di richiesta: la parte della richiesta Web per ispezionare, ad esempio, una stringa di query o il corpo. Per informazioni sui componenti della richiesta Web, vedereComponenti delle richieste Web.

  Una dichiarazione di vincolo di dimensione controlla solo la dimensione del componente dopo l'applicazione di eventuali trasformazioni. Non ispeziona il contenuto del componente.

- Trasformazioni di testo opzionali: trasformazioni che si desidera AWS WAF eseguire sul componente richiesto prima di controllarne le dimensioni. Ad esempio, potete comprimere gli spazi bianchi o decodificare le entità HTML. Se specificate più di una trasformazione, le AWS WAF elabora nell'ordine elencato. Per informazioni, consulta Trasformazioni di testo.

Inoltre, questa istruzione richiede le seguenti impostazioni:

- Condizione di corrispondenza delle dimensioni: indica l'operatore di confronto numerico da utilizzare per confrontare la dimensione fornita con il componente di richiesta che hai scelto. Scegli l'operatore dall'elenco.
- Dimensione: l'impostazione della dimensione, in byte, da utilizzare nel confronto.

Dove trovare questa dichiarazione sulle regole

- Generatore di regole sulla console: per il tipo Match, nella condizione Size match, scegli la condizione che desideri utilizzare.
- API: SizeConstraintStatement

Istruzione regola attacco SQL Injection

Un'istruzione SQL Injection Rule verifica la presenza di codice SQL dannoso. Gli aggressori inseriscono codice SQL dannoso nelle richieste Web per eseguire operazioni come modificare il database o estrarre dati da esso.

Nestable: puoi annidare questo tipo di istruzione.

WCU: il costo base dipende dall'impostazione del livello di sensibilità per la dichiarazione della regola: Low costa 20 e High costa 30.

Se utilizzi il componente di richiesta Tutti i parametri di interrogazione, aggiungi 10 WCU. Se utilizzi il corpo JSON del componente di richiesta, raddoppia il costo base delle WCU. Per ogni trasformazione di testo che applichi, aggiungi 10 WCU.

Questo tipo di istruzione funziona su un componente di richiesta Web e richiede le seguenti impostazioni del componente di richiesta:

- Componente di richiesta: la parte della richiesta Web per ispezionare, ad esempio, una stringa di query o il corpo.

> **Warning**
>
> Se ispezionate i componenti della richiesta Body, JSON body, Headers o Cookies, leggete le limitazioni relative alla quantità di contenuto AWS WAF che può essere ispezionata. Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF

Per informazioni sui componenti della richiesta Web, consulta. Componenti delle richieste Web

- Trasformazioni di testo opzionali: trasformazioni che si desidera AWS WAF eseguire sul componente della richiesta prima di esaminarlo. Ad esempio, potete trasformare in lettere minuscole o normalizzare lo spazio bianco. Se specificate più di una trasformazione, le AWS WAF elabora nell'ordine elencato. Per informazioni, consulta Trasformazioni di testo.

Inoltre, questa dichiarazione richiede la seguente impostazione:

- Livello di sensibilità: questa impostazione regola la sensibilità dei criteri di corrispondenza dell'iniezione SQL. Le opzioni sono LOW e HIGH. L'impostazione predefinita è LOW.

  L'HIGHimpostazione rileva più attacchi di SQL injection ed è l'impostazione consigliata. A causa della maggiore sensibilità, questa impostazione genera un numero maggiore di falsi positivi, soprattutto se le richieste Web contengono in genere stringhe insolite. Durante il test e l'ottimizzazione dell'ACL web, potrebbe essere necessario fare più lavoro per mitigare i falsi positivi. Per informazioni, consulta Test e ottimizzazione delle protezioni AWS WAF.

  L'impostazione inferiore fornisce un rilevamento delle SQL injection meno rigoroso, che comporta anche un minor numero di falsi positivi. LOWpuò essere una scelta migliore per le risorse che dispongono di altre protezioni contro gli attacchi di SQL injection o che hanno una bassa tolleranza ai falsi positivi.

Dove trovare questa dichiarazione di regole

- Generatore di regole sulla console: per il tipo Match, scegli Attack match condition > Contiene attacchi SQL injection.
- API — SqliMatchStatement

Istruzione regola di corrispondenza stringa

Un'istruzione string match indica la stringa che si AWS WAF desidera cercare in una richiesta, dove nella richiesta effettuare la ricerca e come. Ad esempio, puoi cercare una stringa specifica all'inizio di qualsiasi stringa di query nella richiesta o come una corrispondenza esatta per l'intestazione `User-agent` della richiesta. In genere, la stringa è costituita da caratteri ASCII stampabili, ma puoi utilizzare qualsiasi carattere esadecimale da 0x00 a 0xFF (decimale da 0 a 255).

Nestable: puoi annidare questo tipo di istruzione.

WCU: il costo base dipende dal tipo di match utilizzato.

- Corrisponde esattamente alla stringa — 2
- Inizia con string — 2
- Termina con una stringa — 2
- Contiene una stringa — 10
- Contiene la parola — 10

Se si utilizza il componente di richiesta Tutti i parametri di interrogazione, aggiungere 10 WCU. Se utilizzi il corpo JSON del componente di richiesta, raddoppia il costo base delle WCU. Per ogni trasformazione di testo che applichi, aggiungi 10 WCU.

Questo tipo di istruzione funziona su un componente di richiesta Web e richiede le seguenti impostazioni del componente di richiesta:

- Componente di richiesta: la parte della richiesta Web per ispezionare, ad esempio, una stringa di query o il corpo.

  > **Warning**
  >
  > Se ispezionate i componenti della richiesta Body, JSON body, Headers o Cookies, leggete le limitazioni relative alla quantità di contenuto AWS WAF che può essere ispezionata. Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF

  Per informazioni sui componenti della richiesta Web, consulta. Componenti delle richieste Web
- Trasformazioni di testo opzionali: trasformazioni che si desidera AWS WAF eseguire sul componente della richiesta prima di esaminarlo. Ad esempio, potete trasformare in lettere

minuscole o normalizzare lo spazio bianco. Se specificate più di una trasformazione, le AWS WAF elabora nell'ordine elencato. Per informazioni, consulta Trasformazioni di testo.

Inoltre, questa istruzione richiede le seguenti impostazioni:

- Stringa da abbinare: questa è la stringa che AWS WAF desideri confrontare con il componente di richiesta specificato. In genere, la stringa è costituita da caratteri ASCII stampabili, ma puoi utilizzare qualsiasi carattere esadecimale da 0x00 a 0xFF (decimale da 0 a 255).
- Condizione di corrispondenza della stringa: indica il tipo di ricerca che si AWS WAF desidera eseguire.
  - Corrisponde esattamente alla stringa: la stringa e il valore del componente di richiesta sono identici.
  - Inizia con una stringa: la stringa viene visualizzata all'inizio del componente di richiesta.
  - Termina con una stringa: la stringa viene visualizzata alla fine del componente di richiesta.
  - Contiene una stringa: la stringa viene visualizzata in qualsiasi punto del componente della richiesta.
  - Contiene una parola: la stringa specificata deve apparire nel componente di richiesta. Per questa opzione, le stringhe specificate devono contenere solo caratteri alfanumerici o di sottolineatura (A-Z, a-z, 0-9 o _).

    Una delle seguenti condizioni deve essere vera perché la richiesta corrisponda:

    - La stringa corrisponde esattamente al valore del componente di richiesta, ad esempio il valore di un'intestazione.
    - La stringa si trova all'inizio del componente di richiesta ed è seguita da un carattere diverso da un carattere alfanumerico o un carattere di sottolineatura (_), ad esempio, `BadBot;`.
    - La stringa si trova al termine del componente di richiesta ed è preceduta da un carattere diverso da un carattere alfanumerico o un carattere di sottolineatura (_), ad esempio, `;BadBot`.
    - La stringa si trova al centro del componente di richiesta ed è preceduta e seguita da caratteri diversi da caratteri alfanumerici o caratteri di sottolineatura (_), ad esempio, `-BadBot;`.

Dove trovare questa dichiarazione sulla regola

- Generatore di regole sulla console: per il tipo di partita, scegli String match condition, quindi inserisci le stringhe con cui vuoi abbinare.

- API: ByteMatchStatement

Istruzione regola di attacco di Cross-site scripting

Un'istruzione di attacco XSS (cross-site scripting) verifica la presenza di script dannosi in un componente di richiesta Web. In un attacco XSS, l'aggressore sfrutta le vulnerabilità di un sito Web innocuo per iniettare script dannosi del sito client in altri browser Web legittimi.

Nestable: puoi annidare questo tipo di istruzione.

WCU: 40 WCU, come costo base. Se utilizzi il componente di richiesta Tutti i parametri di interrogazione, aggiungi 10 WCU. Se utilizzi il corpo JSON del componente di richiesta, raddoppia il costo base delle WCU. Per ogni trasformazione di testo che applichi, aggiungi 10 WCU.

Questo tipo di istruzione funziona su un componente di richiesta Web e richiede le seguenti impostazioni del componente di richiesta:

- Componente di richiesta: la parte della richiesta Web per ispezionare, ad esempio, una stringa di query o il corpo.

  > **Warning**
  >
  > Se ispezionate i componenti della richiesta Body, JSON body, Headers o Cookies, leggete le limitazioni relative alla quantità di contenuto AWS WAF che può essere ispezionata. Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF

  Per informazioni sui componenti della richiesta Web, consulta. Componenti delle richieste Web
- Trasformazioni di testo opzionali: trasformazioni che si desidera AWS WAF eseguire sul componente della richiesta prima di esaminarlo. Ad esempio, potete trasformare in lettere minuscole o normalizzare lo spazio bianco. Se specificate più di una trasformazione, le AWS WAF elabora nell'ordine elencato. Per informazioni, consulta Trasformazioni di testo.

Dove trovare questa dichiarazione di regole

- Generatore di regole sulla console: per il tipo Match, scegli Attack match condition > Contiene attacchi di iniezione XSS.
- API — XssMatchStatement

Dichiarazioni di regole logiche

Utilizza le istruzioni delle regole logiche per combinare altre istruzioni o annullarne i risultati. Ogni istruzione regola logica accetta almeno un'istruzione nidificata.

Per combinare o negare logicamente i risultati delle istruzioni delle regole, le istruzioni vengono annidate sotto istruzioni di regole logiche.

Le istruzioni con regole logiche sono annidabili. È possibile inserirle all'interno di altre istruzioni di regole logiche e utilizzarle in istruzioni di tipo scope-down. Per informazioni sulle istruzioni scope-down, vedere. Dichiarazioni delimitate

> **Note**
>
> L'editor visivo sulla console supporta un livello di nidificazione delle istruzioni regola, che funziona per molte esigenze. Per annidare più livelli, modifica la rappresentazione JSON della regola sulla console o usa le API.

Questa tabella descrive le istruzioni delle regole logiche e fornisce linee guida per il calcolo dell'utilizzo delle Web ACL Capacity Unit (WCU) per ciascuna di esse. Per informazioni sulle WCU, consulta AWS WAF unità di capacità Web ACL (WCU).

Istruzione logica	Descrizione	WCU
Logica AND	Combina istruzioni annidate con la logica. AND	Basata su istruzioni nidificate
Logica NOT	Nega i risultati di un'istruzione nidificata.	Basata su istruzione nidificata
Logica OR	Combina le istruzioni annidate con OR la logica.	Basata su istruzioni nidificate

ANDdichiarazione delle regole

L'istruzione della AND regola combina le istruzioni annidate con un'ANDoperazione logica, quindi tutte le istruzioni annidate devono corrispondere affinché l'ANDistruzione corrisponda. Ciò richiede almeno un'istruzione nidificata.

Nestable: è possibile annidare questo tipo di istruzione.

wCus: dipende dalle istruzioni annidate.

Dove trovare questa dichiarazione sulle regole

- Generatore di regole sulla console: per Se una richiesta, scegli corrisponde a tutte le istruzioni (AND), quindi compila le istruzioni annidate.
- API — AndStatement

Esempi

L'elenco seguente mostra l'uso di istruzioni di regole AND NOT logiche per eliminare i falsi positivi dalle corrispondenze di un'istruzione di attacco SQL injection. Per questo esempio, supponiamo di poter scrivere un'istruzione di corrispondenza a byte singolo per soddisfare le richieste che generano falsi positivi.

L'istruzione AND corrisponde alle richieste che non corrispondono all'istruzione byte match e che corrispondono all'istruzione di attacco SQL injection.

```
{
      "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"
      }
    }
```

Utilizzando l'editor visivo delle regole della console, è possibile annidare un'istruzione non logica o un'NOTistruzione sotto un'istruzione OR orAND. L'annidamento dell'NOTistruzione è illustrato nell'esempio precedente.

Utilizzando l'editor visivo delle regole della console, è possibile annidare la maggior parte delle istruzioni nestable in un'istruzione di regole logiche, come quella mostrata nell'esempio precedente. Non è possibile utilizzare l'editor visivo per nidificare OR le AND istruzioni. Per configurare questo tipo di nesting, devi fornire la dichiarazione della regola in JSON. Ad esempio, il seguente elenco di regole JSON include un'ORistruzione annidata all'interno di un'istruzione. 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"
  }
}
```

NOTdichiarazione delle regole

L'istruzione della NOT regola nega logicamente i risultati di una singola istruzione annidata, quindi le istruzioni annidate non devono corrispondere affinché l'NOTistruzione corrisponda e viceversa. Ciò richiede un'istruzione nidificata.

Ad esempio, se desideri bloccare le richieste che non provengono da un paese specifico, crea un'NOTistruzione con l'azione impostata su block e annida un'istruzione di corrispondenza geografica che specifichi il paese.

Nestable: puoi annidare questo tipo di istruzione.

wCus: dipende dall'istruzione annidata.

Dove trovare questa dichiarazione sulle regole

- Generatore di regole sulla console: per Se una richiesta, choose non corrisponde all'istruzione (NOT), quindi compila l'istruzione annidata.
- API: NotStatement

ORdichiarazione delle regole

L'istruzione della OR regola combina le istruzioni annidate con OR la logica, quindi una delle istruzioni annidate deve corrispondere affinché l'ORistruzione corrisponda. Ciò richiede almeno un'istruzione nidificata.

Ad esempio, se desideri bloccare le richieste che provengono da un paese specifico o che contengono una stringa di query specifica, puoi creare un'ORistruzione e inserirvi un'istruzione geo match per il paese e un'istruzione di corrispondenza tra stringhe per la stringa di query.

Se invece desideri bloccare le richieste che non provengono da un paese specifico o che contengono una stringa di query specifica, devi modificare l'ORistruzione precedente per annidare l'istruzione geo match un livello più in basso, all'interno di un'NOTistruzione. Questo livello di nidificazione richiede l'utilizzo della formattazione JSON, poiché la console supporta solo un livello di nidificazione.

Nestable: puoi annidare questo tipo di istruzione.

wCus: dipende dalle istruzioni annidate.

Dove trovare questa dichiarazione sulle regole

- Generatore di regole sulla console: per Se una richiesta, scegli corrisponde ad almeno una delle istruzioni (OR), quindi compila le istruzioni annidate.
- API — OrStatement

Esempi

L'elenco seguente mostra l'uso di OR per combinare altre due istruzioni. L'ORistruzione corrisponde se una delle istruzioni annidate corrisponde.

```
{
  "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"
          }
        }
      ]
    }
  }
}
```

Utilizzando l'editor visivo delle regole della console, è possibile annidare la maggior parte delle istruzioni nestable in un'istruzione di regole logiche, ma non è possibile utilizzare l'editor visivo per OR nidificare le istruzioni. AND Per configurare questo tipo di nesting, devi fornire la dichiarazione della regola in JSON. Ad esempio, il seguente elenco di regole JSON include un'ORistruzione annidata all'interno di un'istruzione. 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"
  }
}
```

Istruzione regola basata sulla frequenza

Una regola basata sulla tariffa conta le richieste in entrata e le richieste con limiti di velocità quando arrivano a una velocità troppo elevata. La regola aggrega le richieste in base ai criteri dell'utente e conta e limita i raggruppamenti aggregati in base alla finestra di valutazione della regola, al limite di richieste e alle impostazioni di azione.

> **Note**
>
> Puoi anche limitare la frequenza delle richieste Web utilizzando il livello di protezione mirato del gruppo di regole Bot Control AWS Managed Rules. L'utilizzo di questo gruppo di regole gestito comporta costi aggiuntivi. Per ulteriori informazioni, consulta Opzioni per la limitazione della velocità nelle regole basate sulla velocità e nelle regole mirate di Bot Control.

AWS WAF tiene traccia e gestisce le richieste Web separatamente per ogni istanza di una regola basata sulla tariffa utilizzata. Ad esempio, se si forniscono le stesse impostazioni delle regole basate sulla tariffa in due ACL Web, ciascuna delle due istruzioni della regola rappresenta un'istanza distinta della regola basata sulla tariffa e ciascuna riceve il proprio monitoraggio e gestione da. AWS WAF Se si definisce una regola basata sulla tariffa all'interno di un gruppo di regole e quindi si utilizza tale gruppo di regole in più posizioni, ogni utilizzo crea un'istanza distinta della regola basata sulla tariffa che ottiene il proprio monitoraggio e la propria gestione. AWS WAF

Not nestable: non puoi annidare questo tipo di istruzione all'interno di altre istruzioni. Puoi includerlo direttamente in un ACL Web o in un gruppo di regole.

Istruzione scope-down: questo tipo di regola può utilizzare un'istruzione con estensione decrescente, per restringere l'ambito delle richieste monitorate dalla regola e dei limiti di velocità.

L'istruzione scope-down può essere facoltativa o obbligatoria, a seconda delle altre impostazioni di configurazione delle regole. I dettagli sono descritti in questa sezione. Per informazioni generali sulle istruzioni scope-down, vedere. Dichiarazioni delimitate

WCU: 2, come costo base. Per ogni chiave di aggregazione personalizzata specificata, aggiungi 30 WCU. Se utilizzi un'istruzione scope-down nella regola, calcola e aggiungi le WCU corrispondenti.

Dove trovare questa dichiarazione sulla regola

- Generatore di regole nell'ACL Web, sulla console: in Regola, per Tipo, scegli Regola basata sulla tariffa.
- API: RateBasedStatement

Argomenti

- Impostazioni di alto livello delle regole basate sulla tariffa
- Avvertenze sulle regole basate sulle tariffe
- Opzioni e chiavi di aggregazione
- Istanze e conteggi di aggregazione
- Richiedi un comportamento di limitazione della velocità
- Esempi di regole basate sulla tariffa
- Elenco degli indirizzi IP la cui velocità è limitata da regole basate sulla velocità

Impostazioni di alto livello delle regole basate sulla tariffa

Una dichiarazione di regole basata sulla tariffa utilizza le seguenti impostazioni di alto livello:

- Finestra di valutazione: la quantità di tempo, in secondi, da AWS WAF includere nel conteggio delle richieste, in base all'ora corrente. Ad esempio, per un'impostazione di 120, quando AWS WAF controlla la frequenza, conta le richieste per i 2 minuti immediatamente precedenti l'ora corrente. Le impostazioni valide sono 60 (1 minuto), 120 (2 minuti), 300 (5 minuti) e 600 (10 minuti) e 300 (5 minuti) è l'impostazione predefinita.

  Questa impostazione non determina la frequenza con cui viene verificata la frequenza di AWS WAF controllo della frequenza, ma la distanza con cui viene effettuata ogni volta che viene effettuata la verifica. AWS WAF controlla frequentemente la frequenza, con una tempistica indipendente dall'impostazione della finestra di valutazione.

- Limite di frequenza: il numero massimo di richieste che soddisfano i criteri specificati e che AWS WAF deve essere registrato solo per la finestra di valutazione specificata. L'impostazione del limite minimo consentita è 100. Quando questo limite viene superato, AWS WAF applica l'impostazione dell'azione della regola alle richieste aggiuntive che soddisfano i criteri specificati.

  AWS WAF applica un limite di velocità vicino al limite impostato, ma non garantisce l'esatta corrispondenza del limite. Per ulteriori informazioni, consulta Avvertenze relative alle regole basate sulla tariffa.
- Aggregazione delle richieste: i criteri di aggregazione da utilizzare sul Web richiedono che la regola basata sulla tariffa contenga e limiti di velocità. Il limite di velocità impostato si applica a ogni istanza di aggregazione. Per informazioni dettagliate, consulta Opzioni e chiavi di aggregazione e Istanze e conteggi di aggregazione.
- Azione: l'azione da intraprendere in risposta alle richieste che la regola limita la velocità. È possibile utilizzare qualsiasi azione della regola tranneAllow. Viene impostata come di consueto a livello di regola, ma presenta alcune restrizioni e comportamenti specifici delle regole basate sulle tariffe. Per informazioni generali sulle azioni delle regole, vedere. Operazione delle regole Per informazioni specifiche sulla limitazione della velocità, Richiedi un comportamento di limitazione della velocità consulta questa sezione.
- Ambito di ispezione e limitazione della tariffa: è possibile restringere l'ambito delle richieste registrate nell'informativa basata sulla tariffa e dei limiti di tariffa aggiungendo un riepilogo decrescente. Se si specifica un'istruzione scope-down, la regola aggrega, conta e limita solo le richieste che corrispondono all'istruzione scope-down. Se scegli l'opzione di aggregazione delle richieste Count all, è necessaria l'istruzione scope-down. Per ulteriori informazioni sulle istruzioni scope-down, vedere. Dichiarazioni delimitate
- (Facoltativo) Configurazione IP inoltrata: viene utilizzata solo se si specifica l'indirizzo IP nell'intestazione nell'aggregazione della richiesta, da solo o come parte delle impostazioni delle chiavi personalizzate. AWS WAF recupera il primo indirizzo IP nell'intestazione specificata e lo utilizza come valore di aggregazione. Un'intestazione comune per questo scopo è`X-Forwarded-For`, ma è possibile specificare qualsiasi intestazione. Per ulteriori informazioni, consulta Indirizzo IP inoltrato.

Avvertenze sulle regole basate sulle tariffe

AWS WAF la limitazione della velocità è progettata per controllare le alte percentuali di richieste e proteggere la disponibilità dell'applicazione nel modo più efficiente ed efficace possibile. Non è concepito per una limitazione precisa della frequenza delle richieste.

- AWS WAF stima il tasso di richieste corrente utilizzando un algoritmo che dà maggiore importanza alle richieste più recenti. Per questo motivo, AWS WAF applicherà un limite di velocità vicino al limite impostato, ma non garantisce una corrispondenza esatta del limite.
- Ogni volta che viene AWS WAF stimata la frequenza delle richieste, AWS WAF esamina il numero di richieste pervenute durante la finestra di valutazione configurata. A causa di questo e di altri fattori, come i ritardi di propagazione, è possibile che le richieste arrivino a una frequenza troppo elevata per diversi minuti prima che vengano AWS WAF rilevate e limitate. Allo stesso modo, la frequenza di richiesta può rimanere inferiore al limite per un periodo di tempo prima che AWS WAF rilevi la diminuzione e interrompa l'azione di limitazione della velocità. Di solito, questo ritardo è inferiore a 30 secondi.
- Se modifichi una qualsiasi delle impostazioni del limite di velocità in una regola in uso, la modifica ripristina i conteggi dei limiti di velocità della regola. Ciò può sospendere le attività di limitazione della velocità della regola per un massimo di un minuto. Le impostazioni del limite di velocità sono la finestra di valutazione, il limite di velocità, le impostazioni di aggregazione delle richieste, la configurazione IP inoltrata e l'ambito dell'ispezione.

Opzioni e chiavi di aggregazione

Per impostazione predefinita, una regola basata sulla velocità aggrega e limita la velocità delle richieste in base all'indirizzo IP della richiesta. È possibile configurare la regola per utilizzare diverse altre chiavi di aggregazione e combinazioni di tasti. Ad esempio, è possibile eseguire l'aggregazione in base a un indirizzo IP inoltrato, al metodo HTTP o a un argomento di query. Puoi anche specificare combinazioni di chiavi di aggregazione, come l'indirizzo IP e il metodo HTTP, o i valori di due cookie diversi.

> **Note**
>
> Tutti i componenti della richiesta specificati nella chiave di aggregazione devono essere presenti in una richiesta Web affinché la richiesta venga valutata o la frequenza sia limitata dalla regola.

Puoi configurare la tua regola basata sulla tariffa con le seguenti opzioni di aggregazione.

- Indirizzo IP di origine: aggregazione utilizzando solo l'indirizzo IP dall'origine della richiesta Web.

L'indirizzo IP di origine potrebbe non contenere l'indirizzo del client di origine. Se una richiesta web passa attraverso uno o più proxy o sistemi di bilanciamento del carico, questo conterrà l'indirizzo dell'ultimo proxy.

- Indirizzo IP nell'intestazione: aggregazione utilizzando solo un indirizzo client in un'intestazione HTTP. Questo viene anche chiamato indirizzo IP inoltrato.

  Con questa configurazione, si specifica anche un comportamento di fallback da applicare a una richiesta Web con un indirizzo IP non valido nell'intestazione. Il comportamento di fallback imposta il risultato corrispondente per la richiesta, in modo che corrisponda o non corrisponda. In caso di mancata corrispondenza, la regola basata sulla tariffa non conta né limita la richiesta. Per la corrispondenza, la regola basata sulla frequenza raggruppa la richiesta insieme ad altre richieste con un indirizzo IP non valido nell'intestazione specificata.

  Prestate attenzione con questa opzione, poiché le intestazioni possono essere gestite in modo incoerente dai proxy e possono anche essere modificate per aggirare l'ispezione. Per ulteriori informazioni e procedure consigliate, consulta. Indirizzo IP inoltrato
- Conta tutto: conta e valuta, limita tutte le richieste che corrispondono all'istruzione scope-down della regola. Questa opzione richiede un'istruzione scope-down. In genere viene utilizzato per limitare la velocità di un insieme specifico di richieste, ad esempio tutte le richieste con un'etichetta specifica o tutte le richieste provenienti da un'area geografica specifica.
- Chiavi personalizzate: aggregazione utilizzando una o più chiavi di aggregazione personalizzate. Per combinare una delle opzioni di indirizzo IP con altre chiavi di aggregazione, definiscile qui sotto le chiavi personalizzate.

  Le chiavi di aggregazione personalizzate sono un sottoinsieme delle opzioni del componente di richiesta Web descritte in. Richiedi le opzioni dei componenti

  Le opzioni principali sono le seguenti. Salvo dove indicato, è possibile utilizzare un'opzione più volte, ad esempio due intestazioni o tre namespace di etichette.

  - Label namespace: utilizza uno spazio dei nomi di etichette come chiave di aggregazione. Ogni nome di etichetta completo e distinto che ha lo spazio dei nomi di etichetta specificato contribuisce all'istanza di aggregazione. Se utilizzi solo uno spazio dei nomi di etichette come chiave personalizzata, ogni nome di etichetta definisce completamente un'istanza di aggregazione.

    La regola basata sulla frequenza utilizza solo le etichette che sono state aggiunte alla richiesta da regole che vengono valutate in precedenza nell'ACL Web.

Per informazioni sugli spazi dei nomi e sui nomi delle etichette, vedere. Requisiti per la sintassi e la denominazione delle etichette

- Intestazione: utilizza un'intestazione denominata come chiave di aggregazione. Ogni valore distinto nell'intestazione contribuisce all'istanza di aggregazione.

  L'intestazione richiede una trasformazione del testo opzionale. Per informazioni, consulta Trasformazioni di testo.
- Cookie: utilizza un cookie denominato come chiave di aggregazione. Ogni valore distinto nel cookie contribuisce all'istanza di aggregazione.

  Il cookie richiede una trasformazione del testo opzionale. Per informazioni, consulta Trasformazioni di testo.
- Argomento della query: utilizza un singolo argomento di interrogazione nella richiesta come chiave aggregata. Ogni valore distinto per l'argomento di interrogazione denominato contribuisce all'istanza di aggregazione.

  L'argomento della query richiede una trasformazione del testo opzionale. Per informazioni, consulta Trasformazioni di testo.
- Stringa di query: utilizza l'intera stringa di query nella richiesta come chiave aggregata. Ogni stringa di query distinta contribuisce all'istanza di aggregazione. È possibile utilizzare questo tipo di chiave una sola volta.

  La stringa di query richiede una trasformazione del testo opzionale. Per informazioni, consulta Trasformazioni di testo.
- Percorso URI: utilizza il percorso URI nella richiesta come chiave aggregata. Ogni percorso URI distinto contribuisce all'istanza di aggregazione. È possibile utilizzare questo tipo di chiave una sola volta.

  Il percorso URI richiede una trasformazione del testo opzionale. Per informazioni, consulta Trasformazioni di testo.
- Metodo HTTP: utilizza il metodo HTTP della richiesta come chiave aggregata. Ogni metodo HTTP distinto contribuisce all'istanza di aggregazione. È possibile utilizzare questo tipo di chiave una sola volta.
- Indirizzo IP: aggrega utilizzando l'indirizzo IP dall'origine della richiesta Web in combinazione con altre chiavi.

Potrebbe non contenere l'indirizzo del client di origine. Se una richiesta web passa attraverso uno o più proxy o sistemi di bilanciamento del carico, questo conterrà l'indirizzo dell'ultimo proxy.

- Indirizzo IP nell'intestazione: aggregazione utilizzando l'indirizzo client in un'intestazione HTTP in combinazione con altre chiavi. Questo viene anche chiamato indirizzo IP inoltrato.

  Prestate attenzione con questa opzione, poiché le intestazioni possono essere gestite in modo incoerente dai proxy e possono essere modificate per aggirare l'ispezione. Per ulteriori informazioni e procedure consigliate, consulta. Indirizzo IP inoltrato

Istanze e conteggi di aggregazione

Quando una regola basata sulla tariffa valuta le richieste Web utilizzando i criteri di aggregazione, ogni set univoco di valori trovato dalla regola per le chiavi di aggregazione specificate definisce un'istanza di aggregazione unica.

- Chiavi multiple: se hai definito più chiavi personalizzate, il valore di ciascuna chiave contribuisce alla definizione dell'istanza di aggregazione. Ogni combinazione unica di valori definisce un'istanza di aggregazione.
- Chiave singola: se hai scelto una sola chiave, nelle chiavi personalizzate o selezionando una delle scelte di indirizzo IP di Singleton, ogni valore univoco per la chiave definisce un'istanza di aggregazione.
- Count all - no keys: se hai selezionato l'opzione di aggregazione Count all, tutte le richieste valutate dalla regola appartengono a una singola istanza di aggregazione per la regola. Questa scelta richiede una dichiarazione riassuntiva.

Una regola basata sulla frequenza conta le richieste Web separatamente per ogni istanza di aggregazione che identifica.

Ad esempio, supponiamo che una regola basata sulla frequenza valuti le richieste Web con i seguenti valori di indirizzo IP e metodo HTTP:

- Indirizzo IP 10.1.1.1, metodo HTTP POST
- Indirizzo IP 10.1.1.1, metodo HTTP GET
- Indirizzo IP 127.0.0.0, metodo HTTP POST
- Indirizzo IP 10.1.1.1, metodo HTTP GET

La regola crea diverse istanze di aggregazione in base ai criteri di aggregazione.

- Se il criterio di aggregazione è solo l'indirizzo IP, ogni singolo indirizzo IP è un'istanza di aggregazione e AWS WAF conta le richieste separatamente per ciascuna di esse. I conteggi delle istanze di aggregazione e delle richieste per il nostro esempio sarebbero i seguenti:
  - Indirizzo IP 10.1.1.1: conteggio 3
  - Indirizzo IP 127.0.0.0: numero 1
- Se il criterio di aggregazione è il metodo HTTP, ogni singolo metodo HTTP è un'istanza di aggregazione. Le istanze di aggregazione e i conteggi delle richieste per il nostro esempio sarebbero i seguenti:
  - Metodo HTTP POST: conteggio 2
  - Metodo HTTP GET: conteggio 2
- Se i criteri di aggregazione sono l'indirizzo IP e il metodo HTTP, ogni indirizzo IP e ogni metodo HTTP contribuirebbero all'istanza di aggregazione combinata. Le istanze di aggregazione e i conteggi delle richieste per il nostro esempio sarebbero i seguenti:
  - Indirizzo IP 10.1.1.1, metodo HTTP POST: conteggio 1
  - Indirizzo IP 10.1.1.1, metodo HTTP GET: conteggio 2
  - Indirizzo IP 127.0.0.0, metodo HTTP POST: conteggio 1

Richiedi un comportamento di limitazione della velocità

I criteri AWS WAF utilizzati per limitare la classificazione delle richieste relative a una regola basata sulla tariffa sono gli stessi AWS WAF utilizzati per aggregare le richieste relative alla regola. Se definisci un'istruzione scope-down per la regola, aggrega, conta e limita la velocità AWS WAF solo le richieste che corrispondono all'istruzione scope-down.

I criteri di corrispondenza che fanno sì che una regola basata sulla tariffa applichi le relative impostazioni di azione a una richiesta Web specifica sono i seguenti:

- La richiesta Web corrisponde all'istruzione scope-down della regola, se definita.
- La richiesta Web appartiene a un'istanza di aggregazione il cui numero di richieste è attualmente superiore al limite della regola.

Come AWS WAF si applica l'azione della regola

Quando una regola basata sulla tariffa applica un limite di velocità a una richiesta, applica l'azione della regola e, se hai definito una gestione o un'etichettatura personalizzata nelle specifiche dell'azione, la regola le applica. Questa gestione delle richieste è identica al modo in cui una match rule applica le proprie impostazioni di azione alle richieste web corrispondenti. Una regola basata sulla frequenza applica etichette o esegue altre azioni solo su richieste che limitano attivamente la velocità.

È possibile utilizzare qualsiasi azione della regola tranne. Allow Per informazioni generali sulle azioni delle regole, vedereOperazione delle regole.

L'elenco seguente descrive come funziona la limitazione della velocità per ciascuna delle azioni.

- Block— AWS WAF blocca la richiesta e applica qualsiasi comportamento di blocco personalizzato che hai definito.
- Count— AWS WAF conta la richiesta, applica eventuali intestazioni o etichette personalizzate che hai definito e continua la valutazione ACL web della richiesta.

  Questa azione non limita la frequenza delle richieste. Conta solo le richieste che superano il limite.
- CAPTCHAoppure Challenge: AWS WAF gestisce la richiesta come a Block o come aCount, a seconda dello stato del token della richiesta.

  Questa azione non limita la frequenza di richieste con token validi. Limita la frequenza delle richieste che superano il limite e in cui mancano anche token validi.

  - Se la richiesta non ha un token valido e non scaduto, l'azione blocca la richiesta e invia il CAPTCHA o la sfida del browser al client.

    Se il browser dell'utente finale o del client risponde correttamente, il client riceve un token valido e invia nuovamente la richiesta originale. Se la limitazione della velocità per l'istanza di aggregazione è ancora in vigore, a questa nuova richiesta con il token valido e non scaduto verrà applicata l'azione descritta nel successivo bullet point.
  - Se la richiesta ha un token valido e non scaduto, l'Challengeazione CAPTCHA or verifica il token e non esegue alcuna azione sulla richiesta, simile all'azione. Count La regola basata sulla frequenza restituisce la valutazione della richiesta all'ACL Web senza intraprendere alcuna azione terminativa e l'ACL Web continua la valutazione della richiesta.

  Per ulteriori informazioni, consulta CAPTCHAe Challenge in AWS WAF.

Se si imposta un limite di velocità, solo l'indirizzo IP o l'indirizzo IP inoltrato.

Quando si configura la regola per limitare la velocità solo all'indirizzo IP per l'indirizzo IP inoltrato, l'istanza della regola può limitare la velocità fino a 10.000 indirizzi IP. Se un'istanza della regola identifica più di 10.000 indirizzi IP per il limite di velocità, limita solo i 10.000 mittenti più alti.

Con questa configurazione, è possibile recuperare l'elenco di indirizzi IP attualmente limitati da una regola basata sulla velocità. Se utilizzi un'istruzione scope-down, le richieste a velocità limitata sono solo quelle nell'elenco IP che corrispondono all'istruzione scope-down. Per informazioni sul recupero dell'elenco di indirizzi IP, consulta. Elenco degli indirizzi IP la cui velocità è limitata da regole basate sulla velocità

Esempi di regole basate sulla tariffa

Questa sezione descrive configurazioni di esempio per una serie di casi d'uso comuni di regole basate sulla tariffa.

Ogni esempio fornisce una descrizione del caso d'uso e quindi mostra la soluzione negli elenchi JSON per le regole configurate personalizzate.

> **Note**
>
> Gli elenchi JSON mostrati in questi esempi sono stati creati nella console configurando la regola e quindi modificandola utilizzando l'editor Rule JSON.

Argomenti

- Rate limita le richieste a una pagina di accesso
- Rate limita le richieste a una pagina di accesso da qualsiasi indirizzo IP, coppia di agenti utente
- Rate limita le richieste a cui manca un'intestazione specifica
- Rate, limita le richieste con etichette specifiche
- Rate limita le richieste di etichette con uno spazio dei nomi di etichette specificato

Rate limita le richieste a una pagina di accesso

Per limitare il numero di richieste alla pagina di accesso del tuo sito web senza influire sul traffico verso il resto del sito, puoi creare una regola basata sulla frequenza con un'istruzione scope-down che abbini le richieste alla tua pagina di accesso e con l'aggregazione delle richieste impostata su Count all.

La regola basata sulla frequenza conterà tutte le richieste per la pagina di accesso in un'unica istanza di aggregazione e applicherà l'azione della regola quando le richieste superano il limite.

Il seguente elenco JSON mostra un esempio di questa configurazione di regole. L'opzione di aggregazione count all è elencata in JSON come impostazione. `CONSTANT` Questo esempio corrisponde alle pagine di accesso che iniziano 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
            }
          ]
        }
      }
    }
  }
}
```

Rate limita le richieste a una pagina di accesso da qualsiasi indirizzo IP, coppia di agenti utente

Per limitare il numero di richieste di indirizzo IP alla pagina di accesso del tuo sito Web, imposta l'aggregazione delle richieste su Chiavi personalizzate e fornisci i criteri di aggregazione.

Il seguente elenco JSON mostra un esempio di questa configurazione di regole. In questo esempio, abbiamo impostato il limite a 100 richieste in un periodo di cinque minuti per indirizzo IP, coppia di agenti utente.

```
{
  "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
            }
          ]
        }
      }
    }
  }
}
```

Rate limita le richieste a cui manca un'intestazione specifica

Per limitare il numero di richieste a cui manca un'intestazione specifica, puoi utilizzare l'opzione di aggregazione Count all con un'istruzione scope-down. Configura l'istruzione scope-down con un'istruzione logica contenente un'N0Tistruzione che restituisca true solo se l'intestazione esiste e ha un valore.

Il seguente elenco JSON mostra un esempio di questa configurazione di regole.

```
{
  "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
                }
              ]
            }
          }
        }
      }
    }
  }
}
```

Rate, limita le richieste con etichette specifiche

È possibile combinare la limitazione della velocità con qualsiasi regola o gruppo di regole che aggiunga etichette alle richieste, per limitare il numero di richieste di varie categorie. A tale scopo, configurate il vostro ACL web come segue:

- Aggiungi le regole o i gruppi di regole che aggiungono etichette e configurali in modo che non blocchino o consentano le richieste per le quali desideri limitare la frequenza. Se utilizzi gruppi di regole gestiti, potresti dover sovrascrivere alcune azioni delle regole dei gruppi di regole per Count ottenere questo comportamento.
- Aggiungi una regola basata sulla tariffa all'ACL Web con un'impostazione del numero di priorità superiore alle regole di etichettatura e ai gruppi di regole. AWS WAF valuta le regole in ordine numerico, a partire dalla più bassa, in modo che la regola basata sulla tariffa venga eseguita dopo le regole di etichettatura. Configura la limitazione della velocità sulle etichette utilizzando una combinazione tra la corrispondenza delle etichette nell'istruzione scope-down della regola e l'aggregazione delle etichette.

L'esempio seguente utilizza il gruppo di regole AWS Managed Rules dell'elenco di reputazione IP di Amazon. La regola del gruppo di regole `AWSManagedIPDDoSList` rileva ed etichetta le richieste i cui IP sono noti per essere coinvolti attivamente in attività DDoS. L'azione della regola è configurata Count in base alla definizione del gruppo di regole. Per ulteriori informazioni sul gruppo di regole, vederethe section called “Elenco reputazione IP Amazon”.

Il seguente elenco Web ACL JSON utilizza il gruppo di regole di reputazione IP seguito da una regola basata sulla frequenza di abbinamento delle etichette. La regola basata sulla frequenza utilizza un'istruzione scope-down per filtrare le richieste contrassegnate dalla regola del gruppo di regole. L'istruzione della regola basata sulla frequenza aggrega e limita la velocità delle richieste filtrate in base ai relativi indirizzi 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:"
}
```

Rate limita le richieste di etichette con uno spazio dei nomi di etichette specificato

Le regole di livello comune nel gruppo di regole gestito da Bot Control aggiungono etichette per bot di varie categorie, ma bloccano solo le richieste provenienti da bot non verificati. Per informazioni su queste regole, consulta. Elenco delle regole di Bot Control

Se utilizzi il gruppo di regole gestito da Bot Control, puoi aggiungere una limitazione della velocità per le richieste provenienti da singoli bot verificati. Per fare ciò, aggiungi una regola basata sulla frequenza che viene eseguita dopo il gruppo di regole Bot Control e aggrega le richieste in base alle etichette dei nomi dei bot. Specificate la chiave di aggregazione dello spazio dei

nomi Label e impostate la chiave dello spazio dei nomi su. `awswaf:managed:aws:bot-control:bot:name:` Ogni etichetta univoca con lo spazio dei nomi specificato definirà un'istanza di aggregazione. Ad esempio, le etichette `awswaf:managed:aws:bot-control:bot:name:axios` e `awswaf:managed:aws:bot-control:bot:name:curl` ognuna definiscono un'istanza di aggregazione.

Il seguente elenco Web ACL JSON mostra questa configurazione. La regola in questo esempio limita le richieste per ogni singola istanza di aggregazione di bot a 1.000 in un periodo di due minuti.

```
{
  "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:"
}
```

Elenco degli indirizzi IP la cui velocità è limitata da regole basate sulla velocità

Se la regola basata sulla tariffa si basa solo sull'indirizzo IP o sull'indirizzo IP inoltrato, puoi recuperare l'elenco di indirizzi IP a cui la regola attualmente limita la velocità. AWS WAF memorizza questi indirizzi IP nell'elenco delle chiavi gestite della regola.

> **Note**
>
> Questa opzione è disponibile solo se si esegue l'aggregazione solo sull'indirizzo IP o solo su un indirizzo IP in un'intestazione. Se utilizzi l'aggregazione di richieste di chiavi personalizzate, non puoi recuperare un elenco di indirizzi IP a velocità limitata, anche se utilizzi una delle specifiche dell'indirizzo IP nelle tue chiavi personalizzate.

Una regola basata sulla frequenza applica l'azione della regola alle richieste dall'elenco delle chiavi gestite della regola che corrispondono all'istruzione scope-down della regola. Quando una regola non ha un'istruzione scope-down, applica l'azione a tutte le richieste provenienti dagli indirizzi IP presenti nell'elenco. L'azione della regola è Block predefinita, ma può essere qualsiasi azione valida tranne. Allow Il numero massimo di indirizzi IP che AWS WAF possono limitare la velocità utilizzando una singola istanza di regola basata sulla velocità è 10.000. Se più di 10.000 indirizzi superano il limite di velocità, AWS WAF limita quelli con le tariffe più elevate.

Puoi accedere all'elenco delle chiavi gestite di una regola basata sulla tariffa utilizzando la CLI, l'API o uno qualsiasi degli SDK. In questo argomento viene descritto l'accesso tramite la CLI e le API. La console non fornisce l'accesso all'elenco in questo momento.

Per l' AWS WAF API, il comando è GetRateBasedStatementManagedKeys.

Per la AWS WAF CLI, il comando è get-rate-based-statement -managed-keys.

Di seguito viene illustrata la sintassi per recuperare l'elenco di indirizzi IP a velocità limitata per una regola basata sulla velocità utilizzata in un ACL Web su una distribuzione 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
```

Di seguito viene illustrata la sintassi per un'applicazione regionale, un'API REST di Amazon API Gateway, un Application Load Balancer, un'API AWS AppSync GraphQL, un pool di utenti Amazon Cognito, un servizio o AWS App Runner un'istanza Verified Access. 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 monitora le richieste Web e gestisce le chiavi in modo indipendente per ogni combinazione unica di ACL web, gruppo di regole opzionale e regola basata sulla frequenza. Ad

esempio, se si definisce una regola basata sulla frequenza all'interno di un gruppo di regole e quindi si utilizza il gruppo di regole in un ACL Web, AWS WAF monitora le richieste Web e gestisce le chiavi per tale ACL Web, la dichiarazione di riferimento del gruppo di regole e l'istanza di regola basata sulla frequenza. Se utilizzi lo stesso gruppo di regole in un secondo ACL Web, AWS WAF monitora le richieste Web e gestisce le chiavi per questo secondo utilizzo in modo completamente indipendente dal primo.

Per una regola basata sulla frequenza che hai definito all'interno di un gruppo di regole, devi fornire il nome dell'istruzione di riferimento del gruppo di regole nella richiesta, oltre al nome ACL web e al nome della regola basata sulla frequenza all'interno del gruppo di regole. Di seguito viene illustrata la sintassi per un'applicazione regionale in cui la regola basata sulla velocità è definita all'interno di un gruppo di regole e il gruppo di regole viene utilizzato in un 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
```

Dichiarazioni sulle regole del gruppo di regole

Le istruzioni delle regole del gruppo di regole non sono annidabili.

Questa sezione descrive le istruzioni delle regole del gruppo di regole che è possibile utilizzare nell'ACL Web. Le unità di capacità ACL Web (WCU) del gruppo di regole vengono impostate dal proprietario del gruppo di regole al momento della creazione. Per informazioni sulle WCU, consulta AWS WAF unità di capacità Web ACL (WCU).

Istruzione gruppo di regole	Descrizione	WCU
Gruppo di regole gestite	Esegue le regole definite nel gruppo di regole gestite specificato. È possibile restringere l'ambito delle richieste valutate dal gruppo di regole aggiungendo un'istruzione scope-down.	Definito dal gruppo di regole, più eventuali WCU aggiuntive per un'istruzione scope-down.

Istruzione gruppo di regole	Descrizione	WCU
	Non è possibile inserire un'istruzione gestita di un gruppo di regole all'interno di nessun altro tipo di istruzione.	
Gruppo di regole	Esegue le regole definite in un gruppo di regole gestito dall'utente. Non è possibile aggiunger e un'istruzione con ambito limitato a una dichiarazione di riferimento di un gruppo di regole per il proprio gruppo di regole. Non è possibile inserire un'istruzione di un gruppo di regole all'interno di un altro tipo di istruzione	Il limite WCU per il gruppo di regole viene definito al momento della creazione.

Istruzione gruppo di regole gestite

L'istruzione regola del gruppo di regole gestite aggiunge un riferimento nell'elenco delle regole ACL Web a un gruppo di regole gestite. Questa opzione non viene visualizzata nelle istruzioni regola sulla console, ma quando utilizzi il formato JSON dell'ACL Web, gli eventuali gruppi di regole gestite aggiunti vengono visualizzati sotto le regole ACL Web come questo tipo.

Un gruppo di regole gestito è un gruppo di regole AWS gestite, la maggior parte dei quali sono gratuiti per AWS WAF i clienti, o un gruppo di regole Marketplace AWS gestito. Ti iscrivi automaticamente ai gruppi di regole AWS Managed Rules a pagamento quando li aggiungi al tuo ACL web. Puoi iscriverti ai gruppi di regole Marketplace AWS gestite tramite Marketplace AWS. Per ulteriori informazioni, consulta Gruppi di regole gestite.

Quando aggiungi un gruppo di regole a un ACL Web, puoi sostituire le azioni delle regole del gruppo con Count o con un'altra azione della regola. Per ulteriori informazioni, consulta Le azioni sostituiscono i gruppi di regole.

È possibile restringere l'ambito delle richieste AWS WAF valutate con il gruppo di regole. A tale scopo, si aggiunge un'istruzione scope-down all'interno dell'istruzione del gruppo di regole. Per informazioni sulle istruzioni scope-down, vedere. Dichiarazioni delimitate Questo può aiutarti a gestire il modo in cui il gruppo di regole influisce sul traffico e a contenere i costi associati al volume di traffico quando utilizzi il gruppo di regole. Per informazioni ed esempi sull'utilizzo delle istruzioni scope-down con il gruppo di regole gestito da AWS WAF Bot Control, consulta. AWS WAF Controllo dei bot

Not nestable: non puoi inserire questo tipo di istruzione all'interno di altre istruzioni e non puoi includerlo in un gruppo di regole. Puoi includerlo direttamente in un'ACL Web.

(Facoltativo) Istruzione scope-down: questo tipo di regola richiede un'istruzione scope-down opzionale, per restringere l'ambito delle richieste valutate dal gruppo di regole. Per ulteriori informazioni, consulta Dichiarazioni delimitate.

wCU: impostato per il gruppo di regole al momento della creazione.

Dove trovare questa dichiarazione sulle regole

- Console: durante il processo di creazione di un ACL Web, nella pagina Aggiungi regole e gruppi di regole, scegli Aggiungi gruppi di regole gestiti, quindi trova e seleziona il gruppo di regole che desideri utilizzare.
- API: ManagedRuleGroupStatement

Istruzione gruppo di regole

L'istruzione regola del gruppo di regole aggiunge un riferimento all'elenco di regole ACL Web in un gruppo di regole gestito dall'utente. Questa opzione non viene visualizzata nelle istruzioni regola sulla console, ma quando utilizzi il formato JSON dell'ACL Web, gli eventuali gruppi di regole aggiunti vengono visualizzati sotto le regole ACL Web come questo tipo. Per informazioni sull'uso dei gruppi di regole, consulta Gestione dei propri gruppi di regole.

Quando aggiungi un gruppo di regole a un ACL Web, puoi sovrascrivere le azioni delle regole del gruppo su Count o su un'altra azione della regola. Per ulteriori informazioni, consulta Le azioni sostituiscono i gruppi di regole.

Not nestable: non puoi inserire questo tipo di istruzione all'interno di altre istruzioni e non puoi includerlo in un gruppo di regole. Puoi includerlo direttamente in un'ACL Web.

WCUs: impostato per il gruppo di regole al momento della creazione.

Dove trovare questa dichiarazione sulle regole

- Console: durante il processo di creazione di un ACL Web, nella pagina Aggiungi regole e gruppi di regole, scegli Aggiungi regole e gruppi di regole personalizzati, Gruppo di regole, quindi aggiungi il gruppo di regole che desideri utilizzare.
- API — RuleGroupReferenceStatement

Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF

AWS WAF non supporta l'ispezione di contenuti molto grandi per il corpo, le intestazioni o i cookie dei componenti di richiesta Web. Il servizio host sottostante ha limiti di numero e dimensione su ciò a cui inoltra per AWS WAF l'ispezione. Ad esempio, il servizio host non invia più di 200 intestazioni AWS WAF, quindi per una richiesta web con 205 intestazioni, non AWS WAF può controllare le ultime 5 intestazioni.

Quando si AWS WAF consente a una richiesta Web di passare alla risorsa protetta, viene inviata l'intera richiesta Web, inclusi tutti i contenuti che non rientrano nei limiti di numero e dimensione consentiti per l'ispezione AWS WAF .

Limiti di dimensione per l'ispezione dei componenti

I limiti di dimensione per l'ispezione dei componenti sono i seguenti:

- **`Body`**e **`JSON Body`** — Per Application Load Balancer and AWS AppSync, AWS WAF può ispezionare i primi 8 KB del corpo di una richiesta. Infatti CloudFront, API Gateway, Amazon Cognito, App Runner e Verified Access, per impostazione predefinita, AWS WAF possono ispezionare i primi 16 KB e puoi aumentare il limite fino a 64 KB nella tua configurazione ACL web. Per ulteriori informazioni, consulta Gestione dei limiti di dimensione delle ispezioni corporee.
- **`Headers`**— AWS WAF può ispezionare al massimo i primi 8 KB (8.192 byte) delle intestazioni di richiesta e al massimo le prime 200 intestazioni. Il contenuto è disponibile per l'ispezione AWS WAF fino al primo limite raggiunto.

- **`Cookies`**— AWS WAF può ispezionare al massimo i primi 8 KB (8.192 byte) dei cookie di richiesta e al massimo i primi 200 cookie. Il contenuto è disponibile per l'ispezione AWS WAF fino al primo limite raggiunto.

Opzioni di gestione sovradimensionate per le istruzioni delle regole

Quando si scrive una dichiarazione di regola che esamina uno di questi tipi di componenti di richiesta, si specifica come gestire i componenti di grandi dimensioni. La gestione di dimensioni eccessive indica AWS WAF cosa fare con una richiesta Web quando il componente di richiesta esaminato dalla regola supera i limiti di dimensione.

Le opzioni per la gestione dei componenti di grandi dimensioni sono le seguenti:

- Continue— Ispeziona normalmente il componente della richiesta in base ai criteri di ispezione delle regole. AWS WAF ispezionerà i contenuti del componente della richiesta che rientrano nei limiti di dimensione.
- Match— Considera la richiesta web come se corrispondesse alla dichiarazione della regola. AWS WAF applica l'azione della regola alla richiesta senza valutarla rispetto ai criteri di ispezione della regola.
- No match— Considera la richiesta web come se non corrispondesse alla dichiarazione della regola senza valutarla rispetto ai criteri di ispezione della regola. AWS WAF continua l'ispezione della richiesta Web utilizzando il resto delle regole dell'ACL Web come farebbe per qualsiasi regola non corrispondente.

Nella AWS WAF console, devi scegliere una di queste opzioni di gestione. All'esterno della console, l'opzione predefinita èContinue.

Se si utilizza l'Matchopzione in una regola la cui azione è impostata suBlock, la regola bloccherà una richiesta il cui componente ispezionato è sovradimensionato. Con qualsiasi altra configurazione, la disposizione finale della richiesta dipende da vari fattori, come la configurazione delle altre regole nell'ACL Web e l'impostazione di azione predefinita dell'ACL Web.

Gestione sovradimensionata in gruppi di regole di cui non sei proprietario

Le limitazioni relative alla dimensione e al numero dei componenti si applicano a tutte le regole utilizzate nell'ACL Web. Ciò include tutte le regole che utilizzi ma non gestisci, nei gruppi di regole gestiti e nei gruppi di regole condivisi con te da un altro account.

Quando utilizzi un gruppo di regole che non gestisci, il gruppo di regole potrebbe avere una regola che esamina un componente di richiesta limitato ma che non gestisce i contenuti di grandi dimensioni nel modo in cui desideri che vengano gestiti. Per informazioni su come AWS Managed Rules gestisce i componenti di grandi dimensioni, consulta. AWS Elenco dei gruppi di regole di Managed Rules Per informazioni su altri gruppi di regole, rivolgiti al fornitore del gruppo di regole.

Linee guida per la gestione di componenti di grandi dimensioni nell'ACL Web

Il modo in cui gestite i componenti di grandi dimensioni nell'ACL Web può dipendere da una serie di fattori, come la dimensione prevista del contenuto del componente della richiesta, la gestione predefinita delle richieste dell'ACL Web e il modo in cui le altre regole dell'ACL Web corrispondono e gestiscono le richieste.

Le linee guida generali per la gestione di componenti di richieste Web di grandi dimensioni sono le seguenti:

- Se devi consentire alcune richieste con contenuti di componenti sovradimensionati, se possibile, aggiungi delle regole per consentire esplicitamente solo quelle richieste. Assegna priorità a tali regole in modo che vengano eseguite prima di qualsiasi altra regola nell'ACL Web che ispeziona gli stessi tipi di componenti. Con questo approccio, non sarete in grado di AWS WAF ispezionare l'intero contenuto dei componenti sovradimensionati che consentite di trasferire alla risorsa protetta.
- Per tutte le altre richieste, puoi impedire il passaggio di byte aggiuntivi bloccando le richieste che superano il limite:
  - Le tue regole e i tuoi gruppi di regole: nelle tue regole che controllano i componenti con limiti di dimensione, configura la gestione delle dimensioni eccessive in modo da bloccare le richieste che superano il limite. Ad esempio, se la tua regola blocca le richieste con contenuti di intestazione specifici, imposta la gestione delle sovradimensionate in modo che corrisponda alle richieste con contenuti di intestazione sovradimensionati. In alternativa, se l'ACL Web blocca le richieste per impostazione predefinita e la regola consente contenuti di intestazione specifici, configura la gestione sovradimensionata della regola in modo che non corrisponda a nessuna richiesta con contenuti di intestazione sovradimensionati.
  - Gruppi di regole che non gestisci: per evitare che i gruppi di regole che non gestisci consentano componenti di richiesta sovradimensionati, puoi aggiungere una regola separata che controlli il tipo di componente della richiesta e blocchi le richieste che superano i limiti. Assegna la priorità alla regola nell'ACL Web in modo che venga eseguita prima dei gruppi di regole. Ad esempio, potete bloccare le richieste con contenuti corporei sovradimensionati prima che qualsiasi

regola di body inspection venga eseguita nell'ACL Web. La procedura seguente descrive come aggiungere questo tipo di regola.

Per aggiungere una regola che blocchi contenuti di grandi dimensioni

1. Quando crei o modifichi il tuo ACL web, nelle impostazioni delle regole, scegli Aggiungi regole, Aggiungi regole e gruppi di regole personalizzati, Generatore di regole, quindi Editor visivo di regole. Per indicazioni sulla creazione o la modifica di un ACL Web, consulta. Utilizzo delle ACL Web
2. Inserisci un nome per la regola e lascia l'impostazione Tipo su Regola normale.
3. Modifica le seguenti impostazioni di partita rispetto a quelle predefinite:
   a. In Statement, per Inspect, apri il menu a discesa e scegli il componente di richiesta web di cui hai bisogno, tra Body, Headers o Cookies.
   b. Per il tipo di partita, scegli Dimensione maggiore di.
   c. In Dimensione, digita un numero che corrisponda almeno alla dimensione minima per il tipo di componente. Per le intestazioni e i cookie, digita`8192`. In Application Load Balancer o negli ACL AWS AppSync Web, per i corpi, digitare. `8192` Per i body in CloudFront API Gateway, Amazon Cognito, App Runner o Verified Access Web ACL, se utilizzi il limite di dimensione corporea predefinito, digita. `16384` Altrimenti, digita il limite di dimensione corporea che hai definito per il tuo ACL web.
   d. Per la gestione delle dimensioni eccessive, seleziona Match.
4. Per Azione, seleziona Blocca.
5. Scegli Aggiungi regola.
6. Dopo aver aggiunto la regola, nella pagina Imposta la priorità delle regole, spostala al di sopra di tutte le regole o i gruppi di regole dell'ACL Web che controllano lo stesso tipo di componente. Ciò le conferisce un'impostazione di priorità numerica inferiore, che fa sì che venga valutata AWS WAF per prima. Per ulteriori informazioni, consulta Ordine di elaborazione delle regole e dei gruppi di regole in un ACL Web.

Corrispondenza dei modelli di espressioni regolari in AWS WAF

AWS WAF supporta la sintassi del pattern usata dalla libreria PCRE. `libpcre` La libreria è documentata in PCRE - Perl Compatible Regular Expressions.

AWS WAF non supporta tutti i costrutti della libreria. Ad esempio, supporta alcune asserzioni a larghezza zero, ma non tutte. Non disponiamo di un elenco completo dei costrutti supportati. Tuttavia, se si fornisce un pattern regex non valido o si utilizzano costrutti non supportati, l' AWS WAF API segnala un errore.

AWS WAF non supporta i seguenti modelli PCRE:

- Backreference e sottoespressioni di acquisizione
- Riferimenti di subroutine e modelli ricorsivi
- Modelli condizionali
- Verbi di controllo di backtracking
- La direttiva\C a byte singolo
- La direttiva \R di corrispondenza nuova riga
- L'inizio \K della direttiva di reimpostazione della corrispondenza
- Callout e codice incorporato
- Raggruppamento atomico e quantificatori possessivi

Set IP e set di pattern regex in AWS WAF

AWS WAF memorizza alcune informazioni più complesse in set che utilizzi facendone riferimento nelle tue regole. Ognuno di questi set dispone di un nome e gli viene assegnato un Amazon Resource Name (ARN) al momento della creazione. Puoi gestire questi set dall'interno delle istruzioni regola e puoi accedervi e gestirli autonomamente tramite il riquadro di navigazione della console.

Incoerenze temporanee durante gli aggiornamenti

Quando si crea o si modifica un ACL Web o altre AWS WAF risorse, le modifiche richiedono poco tempo per essere propagate in tutte le aree in cui sono archiviate le risorse. Il tempo di propagazione può variare da pochi secondi a diversi minuti.

Di seguito sono riportati alcuni esempi delle incongruenze temporanee che potreste notare durante la propagazione delle modifiche:

- Dopo aver creato un ACL Web, se si tenta di associarlo a una risorsa, è possibile che venga visualizzata un'eccezione che indica che l'ACL Web non è disponibile.
- Dopo aver aggiunto un gruppo di regole a un ACL Web, le nuove regole del gruppo di regole potrebbero essere in vigore in un'area in cui viene utilizzato l'ACL Web e non in un'altra.

- Dopo aver modificato l'impostazione di un'azione della regola, è possibile vedere la vecchia azione in alcuni punti e la nuova azione in altri.
- Dopo aver aggiunto un indirizzo IP a un set IP utilizzato in una regola di blocco, il nuovo indirizzo potrebbe essere bloccato in un'area mentre è ancora consentito in un'altra.

Argomenti

Creazione e gestione di un set di IP

Un set di IP fornisce una raccolta di indirizzi IP e intervalli di indirizzi IP che desideri utilizzare insieme in un'istruzione regola. I set IP sono AWS risorse.

Per utilizzare un IP impostato in un ACL Web o in un gruppo di regole, è innanzitutto necessario creare una AWS risorsa `IPSet` con le specifiche dell'indirizzo. Quindi fai riferimento al set quando aggiungi un'istruzione regola del set di IP a un'ACL Web o a un gruppo di regole.

Argomenti

Creazione di un set di IP

Segui la procedura descritta in questa sezione per creare un nuovo set di IP.

> **Note**
>
> Oltre alla procedura in questa sezione, puoi aggiungere un nuovo set di IP quando aggiungi una regola di corrispondenza IP all'ACL Web o al gruppo di regole. Se scegli tale opzione, devi fornire le stesse impostazioni che sono richieste da questa procedura.

Per creare un set di IP

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, scegliere IP sets (Set di IP), quindi Create IP set (Crea set di IP).
3. Immettere un nome e una descrizione per il set di IP. Verranno utilizzati per identificare il set quando richiesto.

   > **Note**
   >
   > Non è possibile modificare il nome dopo aver creato il set di IP.

4. Per Regione, scegli Global (CloudFront) o scegli la regione in cui desideri archiviare il set IP. È possibile utilizzare i set IP regionali solo negli ACL Web che proteggono le risorse regionali. Per utilizzare un IP impostato negli ACL Web che proteggono CloudFront le distribuzioni Amazon, devi utilizzare Global ()CloudFront.
5. In IP version (Versione IP), selezionare la versione che si desidera utilizzare.
6. Nella casella di testo Indirizzi IP, inserisci un indirizzo IP o un intervallo di indirizzi IP per riga, in notazione CIDR. AWS WAF supporta tutti gli intervalli CIDR IPv4 e IPv6 ad eccezione di. `/0` Per ulteriori informazioni sulla notazione CIDR, consulta Supernetting su Wikipedia.

   Ecco alcuni esempi:

   - Per specificare l'indirizzo IPv4 192.0.2.44, digitare 192.0.2.44/32.
   - Per specificare l'indirizzo IPv6 2620:0:2 d 0:200:0:0:0, digitare 2620:0:2 d 0:200:0:0:0 /128.
   - Per specificare l'intervallo di indirizzi IPv4 da 192.0.2.0 a 192.0.2.255, digitare 192.0.2.0/24.
   - Per specificare l'intervallo di indirizzi IPv6 da 2620:0:2d0:200:0:0:0:0 a 2620:0:2d0:200:ffff:ffff:ffff:ffff, immettere 2620:0:2d0:200::/64.
7. Rivedere le impostazioni per il set di IP e scegliere Create IP set (Crea set di IP).

Utilizzo di un set di IP in un gruppo di regole o ACL Web

Per utilizzare un set di IP, aggiungi un'istruzione regola che fa riferimento al gruppo di regole o all'ACL Web in cui è richiesta. Per informazioni, consulta Istruzione regola di corrispondenza set di IP.

Modifica di un set di IP

Per aggiungere o rimuovere indirizzi IP o intervalli di indirizzi IP da un set di IP o modificarne la descrizione, procedi come indicato di seguito.

Per modificare un set di IP

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, selezionare IP sets (Set di IP).
3. Selezionare il set di IP da modificare e scegliere Edit (Modifica).
4. Modificare la versione e gli indirizzi IP in base alle esigenze. Nella casella di testo Indirizzi IP, devi avere un indirizzo IP o un intervallo di indirizzi IP per riga, in notazione CIDR. AWS WAF supporta tutti gli intervalli CIDR IPv4 e IPv6 ad eccezione di. `/0` Per ulteriori informazioni sulla notazione CIDR, consulta Supernetting su Wikipedia. Per gli indirizzi, immettere un indirizzo IP o un intervallo di indirizzi IP per riga, in notazione CIDR.

   Ecco alcuni esempi:

   - Per specificare l'indirizzo IPv4 192.0.2.44, digitare 192.0.2.44/32.
   - Per specificare l'indirizzo IPv6 2620:0:2 d 0:200:0:0:0, digitare 2620:0:2 d 0:200:0:0:0 /128.
   - Per specificare l'intervallo di indirizzi IPv4 da 192.0.2.0 a 192.0.2.255, digitare 192.0.2.0/24.
   - Per specificare l'intervallo di indirizzi IPv6 da 2620:0:2d0:200:0:0:0:0 a 2620:0:2d0:200:ffff:ffff:ffff:ffff, immettere 2620:0:2d0:200::/64.
5. Scegli Save changes (Salva modifiche).

Eliminazione di un set di IP

Segui le linee guida riportate in questa sezione per eliminare un set di riferimento.

Eliminazione di set e gruppi di regole referenziati

Quando si elimina un'entità che è possibile utilizzare in un ACL Web, ad esempio un set di IP, un set di pattern regex o un gruppo di regole, AWS WAF verifica se l'entità è attualmente utilizzata in un ACL Web. Se rileva che è in uso, AWS WAF ti avvisa. AWS WAF è quasi sempre in grado di determinare se un'entità è referenziata da un ACL web. Tuttavia, in rari casi, potrebbe non essere in grado di farlo. Se vuoi essere sicuro che al momento non stia utilizzando l'entità, controllala negli

ACL web prima di eliminarla. Se l'entità è un set di riferimento, controlla anche che nessun gruppo di regole la stia utilizzando.

Per eliminare un set di IP

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, selezionare IP sets (Set di IP).
3. Selezionare il set di IP che si desidera eliminare e scegliere Delete (Elimina).

Creazione e gestione di un set del modello regex

Un set del modello regex fornisce una raccolta di espressioni regolari che desideri utilizzare insieme in un'istruzione regola. I set di pattern Regex sono AWS risorse.

Per utilizzare un pattern regex impostato in un ACL Web o in un gruppo di regole, devi prima creare una AWS risorsa, `RegexPatternSet` con le specifiche del modello regex. Quindi fare riferimento al set quando si aggiunge un'istruzione regola di set del modello regex a un'ACL Web o a un gruppo di regole. Un set del modello regex deve contenere almeno un modello regex.

Se il set di pattern regex contiene più di un pattern regex, quando viene utilizzato in una regola, la corrispondenza dei pattern viene combinata con la logica. `OR` Ovvero, una richiesta Web corrisponderà all'istruzione regola di set del modello se il componente della richiesta corrisponde a uno qualsiasi dei modelli nel set.

AWS WAF supporta la sintassi del pattern utilizzata dalla libreria `libpcre` PCRE con alcune eccezioni. La libreria è documentata in PCRE - Perl Compatible Regular Expressions. Per informazioni sul AWS WAF supporto, vedere. Corrispondenza dei modelli di espressioni regolari in AWS WAF

Argomenti

- Creazione di un set del modello regex
- Utilizzo di un set del modello regex in un gruppo di regole o in un'ACL Web
- Eliminazione di un set del modello regex

Creazione di un set del modello regex

Segui la procedura in questa sezione per creare un nuovo set del modello regex.

Per creare un set del modello regex

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, scegliere Regex pattern sets (Set del modello regex), quindi selezionare Create regex pattern set (Crea set del modello regex).
3. Immettere un nome e una descrizione per il set del modello regex. Verranno utilizzati per identificare il set quando richiesto.

   > **Note**
   >
   > Non è possibile modificare il nome dopo aver creato il set del modello regex.

4. Per Regione, scegli Global (CloudFront) o scegli la regione in cui desideri memorizzare il set di pattern regex. Potete utilizzare i set di pattern regex regionali solo negli ACL Web che proteggono le risorse regionali. Per utilizzare un pattern regex impostato negli ACL Web che proteggono CloudFront le distribuzioni Amazon, devi utilizzare Global (). CloudFront
5. Nella casella di testo Regular expressions (Espressioni regolari), immettere un modello regex per riga.

   Ad esempio, l'espressione regolare `I[a@]mAB[a@]dRequest` corrisponde alle seguenti stringhe: `IamABadRequest`, `IamAB@dRequest`, `I@mABadRequest` e `I@mAB@dRequest`.

   AWS WAF supporta la sintassi del pattern utilizzata dalla libreria PCRE con alcune eccezioni. `libpcre` La libreria è documentata in PCRE - Perl Compatible Regular Expressions. Per informazioni sul AWS WAF supporto, vedere. Corrispondenza dei modelli di espressioni regolari in AWS WAF
6. Rivedere le impostazioni per il set del modello regex e scegliere Create regex pattern set (Crea set del modello regex).

Utilizzo di un set del modello regex in un gruppo di regole o in un'ACL Web

Per utilizzare un set del modello regex in un gruppo di regole o in un'ACL Web, nella console, quando aggiungi o aggiorni le regole nel gruppo di regole o nell'ACL Web, nell'interfaccia Rule builder (Generatore di regole) per Request option (Opzione richiesta), seleziona il componente della richiesta che desideri confrontare con il set del modello. Scegli Match type (Tipo di corrispondenza) > String match condition (Condizione corrispondenza stringa) > Matches pattern from regular expression

(Corrisponde al modello dall'espressione regolare), quindi seleziona il nome del set del modello regex che desideri utilizzare.

Eliminazione di un set del modello regex

Segui le linee guida riportate in questa sezione per eliminare un set di riferimento.

Eliminazione di set e gruppi di regole referenziati

Quando si elimina un'entità che è possibile utilizzare in un ACL Web, ad esempio un set di IP, un set di pattern regex o un gruppo di regole, AWS WAF verifica se l'entità è attualmente utilizzata in un ACL Web. Se rileva che è in uso, AWS WAF ti avvisa. AWS WAF è quasi sempre in grado di determinare se un'entità è referenziata da un ACL web. Tuttavia, in rari casi, potrebbe non essere in grado di farlo. Se vuoi essere sicuro che al momento non stia utilizzando l'entità, controllala negli ACL web prima di eliminarla. Se l'entità è un set di riferimento, controlla anche che nessun gruppo di regole la stia utilizzando.

Per eliminare un set del modello regex

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, scegliere Regex pattern sets (Set del modello regex).
3. Selezionare il set del modello regex da eliminare e scegliere Delete (Elimina).

Richieste e risposte web personalizzate in AWS WAF

È possibile aggiungere un comportamento personalizzato di gestione delle richieste e delle risposte Web alle azioni delle AWS WAF regole e alle azioni ACL Web predefinite. Le tue impostazioni personalizzate si applicano ogni volta che si applica l'azione a cui sono associate.

Puoi personalizzare le richieste e le risposte web nei seguenti modi:

- ConAllow, CountCAPTCHA, e Challenge actions, puoi inserire intestazioni personalizzate nella richiesta web. Quando AWS WAF inoltra la richiesta Web alla risorsa protetta, la richiesta contiene l'intera richiesta originale più le intestazioni personalizzate che hai inserito. Per le Challenge azioni CAPTCHA and, applica la personalizzazione AWS WAF solo se la richiesta supera l'ispezione CAPTCHA o del token di sfida.

- Con Block le azioni, puoi definire una risposta personalizzata completa, con codice di risposta, intestazioni e corpo. La risorsa protetta risponde alla richiesta utilizzando la risposta personalizzata fornita da. AWS WAF La risposta personalizzata sostituisce la risposta all'Blockazione predefinita di. `403 (Forbidden)`

Impostazioni di azione che è possibile personalizzare

È possibile specificare una richiesta o una risposta personalizzata quando si definiscono le seguenti impostazioni di azione:

- Operazione della regola. Per informazioni, consulta Operazione delle regole.
- Azione predefinita per un ACL Web. Per informazioni, consulta L'azione predefinita dell'ACL Web.

Impostazioni di azione che non è possibile personalizzare

Non è possibile specificare una gestione personalizzata delle richieste nell'azione di sostituzione per un gruppo di regole utilizzato in un ACL Web. Per informazioni, consulta Valutazione delle regole ACL Web e dei gruppi di regole. Vedi Istruzione gruppo di regole gestite anche e. Istruzione gruppo di regole

Incoerenze temporanee durante gli aggiornamenti

Quando si crea o si modifica un ACL Web o altre AWS WAF risorse, le modifiche richiedono poco tempo per essere propagate in tutte le aree in cui sono archiviate le risorse. Il tempo di propagazione può variare da pochi secondi a diversi minuti.

Di seguito sono riportati alcuni esempi delle incongruenze temporanee che potreste notare durante la propagazione delle modifiche:

- Dopo aver creato un ACL Web, se si tenta di associarlo a una risorsa, è possibile che venga visualizzata un'eccezione che indica che l'ACL Web non è disponibile.
- Dopo aver aggiunto un gruppo di regole a un ACL Web, le nuove regole del gruppo di regole potrebbero essere in vigore in un'area in cui viene utilizzato l'ACL Web e non in un'altra.
- Dopo aver modificato l'impostazione di un'azione della regola, è possibile vedere la vecchia azione in alcuni punti e la nuova azione in altri.
- Dopo aver aggiunto un indirizzo IP a un set IP utilizzato in una regola di blocco, il nuovo indirizzo potrebbe essere bloccato in un'area mentre è ancora consentito in un'altra.

Limiti all'utilizzo di richieste e risposte personalizzate

AWS WAF definisce le impostazioni massime per l'utilizzo di richieste e risposte personalizzate. Ad esempio, un numero massimo di intestazioni di richiesta per ACL Web o gruppo di regole e un numero massimo di intestazioni personalizzate per una singola definizione di risposta personalizzata. Per informazioni, consulta AWS WAF quote.

Argomenti

- Inserimenti personalizzati nell'intestazione della richiesta per azioni non bloccanti
- Risposte personalizzate per Block le azioni
- Codici di stato supportati per una risposta personalizzata

Inserimenti personalizzati nell'intestazione della richiesta per azioni non bloccanti

Puoi indicare di AWS WAF inserire intestazioni personalizzate nella richiesta HTTP originale quando un'azione della regola non blocca la richiesta. Con questa opzione, puoi solo aggiungere qualcosa alla richiesta. Non puoi modificare o sostituire alcuna parte della richiesta originale. I casi d'uso per l'inserimento di intestazioni personalizzate includono la segnalazione a un'applicazione a valle di elaborare la richiesta in modo diverso in base alle intestazioni inserite e il contrassegno della richiesta per l'analisi.

Questa opzione si applica alle azioni Allow delle regole Challenge e alle azioni Web ACL predefinite su. Count CAPTCHA Allow Per ulteriori informazioni sulle operazioni delle regole, consulta Operazione delle regole. Per ulteriori informazioni sulle azioni ACL Web predefinite, vedere. L'azione predefinita dell'ACL Web

Nomi personalizzati delle intestazioni delle richieste

AWS WAF inserisce come prefisso tutte le intestazioni di richiesta con cui viene inserita`x-amzn-waf-`, per evitare confusione con le intestazioni già presenti nella richiesta. Ad esempio, se si specifica il nome dell'intestazione, inserisce l'intestazione. `sample` AWS WAF `x-amzn-waf-sample`

Intestazioni con lo stesso nome

Se la richiesta ha già un'intestazione con lo stesso nome da inserire, AWS WAF sovrascrive l'intestazione. AWS WAF Pertanto, se si definiscono delle intestazioni in più regole con nomi identici,

l'intestazione dell'ultima regola utilizzata per esaminare la richiesta e trovare una corrispondenza verrebbe aggiunta, a differenza di tutte le regole precedenti.

Intestazioni personalizzate con azioni di regola non terminanti

A differenza dell'Allowazione, l'Countazione non AWS WAF impedisce di elaborare la richiesta Web utilizzando il resto delle regole dell'ACL Web. Allo stesso modo, quando CAPTCHA e Challenge determinano che il token di richiesta è valido, queste azioni non AWS WAF impediscono l'elaborazione della richiesta web. Pertanto, se inserisci intestazioni personalizzate utilizzando una regola con una di queste azioni, anche le regole successive potrebbero inserire intestazioni personalizzate. Per ulteriori informazioni sul comportamento delle regole, vedere. Operazione delle regole

Ad esempio, supponiamo di avere le seguenti regole, con priorità nell'ordine mostrato:

1. Regola A con un'Countazione e un'intestazione personalizzata denominata. `RuleAHeader`
2. RuleB con un'Allowazione e un'intestazione personalizzata denominata. `RuleBHeader`

Se una richiesta corrisponde sia alla regola A che alla regola B, AWS WAF inserisce le intestazioni `x-amzn-waf-RuleAHeader` ex`-amzn-waf-RuleBHeader`, quindi inoltra la richiesta alla risorsa protetta.

AWS WAF inserisce intestazioni personalizzate in una richiesta Web al termine dell'ispezione della richiesta. Pertanto, se si utilizza la gestione personalizzata delle richieste con una regola la cui azione è impostata suCount, le intestazioni personalizzate aggiunte non vengono esaminate dalle regole successive.

Esempio di gestione personalizzata delle richieste

Si definisce la gestione personalizzata delle richieste per l'azione di una regola o per l'azione predefinita di un ACL Web. L'elenco seguente mostra il codice JSON per la gestione personalizzata aggiunto all'azione predefinita per un 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"
 }
}
```

Risposte personalizzate per Block le azioni

Puoi indicare di AWS WAF inviare una risposta HTTP personalizzata al client per le azioni relative alle regole o alle azioni predefinite Web ACL impostate su. Block Per ulteriori informazioni sulle operazioni delle regole, consulta Operazione delle regole. Per ulteriori informazioni sulle azioni ACL Web predefinite, vedere. L'azione predefinita dell'ACL Web

Quando si definisce la gestione personalizzata delle risposte per un'Blockazione, si definiscono il codice di stato, le intestazioni e il corpo della risposta. Per un elenco dei codici di stato che puoi utilizzare AWS WAF, consulta la sezione che segue,Codici di stato supportati per una risposta personalizzata.

Casi d'uso

I casi d'uso per le risposte personalizzate includono quanto segue:

- Invio di un codice di stato non predefinito al client.
- Invio di intestazioni di risposta personalizzate al client. È possibile specificare qualsiasi nome di intestazione ad eccezione di. `content-type`

- Invio di una pagina di errore statica al client.
- Reindirizzamento del client a un URL diverso. A tale scopo, specificate uno dei codici di stato del `3xx` reindirizzamento, ad esempio `301 (Moved Permanently)` o`302 (Found)`, e quindi specificate una nuova intestazione denominata `Location` con il nuovo URL.

Interazione con le risposte definite nella risorsa protetta

Le risposte personalizzate specificate per l' AWS WAF Blockazione hanno la precedenza su tutte le specifiche di risposta definite nella risorsa protetta.

Il servizio host per la AWS risorsa con cui proteggi AWS WAF potrebbe consentire la gestione personalizzata delle risposte per le richieste Web. Considerare i seguenti esempi:

- Con Amazon CloudFront, puoi personalizzare la pagina di errore in base al codice di stato. Per informazioni, consulta Generazione di risposte di errore personalizzate nella Amazon CloudFront Developer Guide.
- Con Amazon API Gateway puoi definire il codice di risposta e di stato per il tuo gateway. Per informazioni, consulta le risposte del gateway in API Gateway nella Amazon API Gateway Developer Guide.

Non puoi combinare impostazioni di risposta AWS WAF personalizzate con impostazioni di risposta personalizzate nella AWS risorsa protetta. Le specifiche di risposta per ogni singola richiesta web provengono completamente AWS WAF o completamente dalla risorsa protetta.

Per le richieste Web che AWS WAF bloccano, quanto segue mostra l'ordine di precedenza.

1. AWS WAF risposta personalizzata: se per l' AWS WAF Blockazione è abilitata una risposta personalizzata, la risorsa protetta invia la risposta personalizzata configurata al client. Qualsiasi impostazione di risposta che potresti aver definito nella risorsa protetta stessa non ha alcun effetto.
2. Risposta personalizzata definita nella risorsa protetta: in caso contrario, se per la risorsa protetta sono state specificate impostazioni di risposta personalizzate, la risorsa protetta utilizza tali impostazioni per rispondere al client.
3. AWS WAF Blockrisposta predefinita: in caso contrario, la risorsa protetta risponde al client con la Block risposta AWS WAF `403 (Forbidden)` predefinita.

Per le richieste Web che lo AWS WAF consentono, la configurazione della risorsa protetta determina la risposta che questa invia al client. Non è possibile configurare le impostazioni di risposta AWS

WAF per le richieste consentite. L'unica personalizzazione che puoi configurare AWS WAF per le richieste consentite è l'inserimento di intestazioni personalizzate nella richiesta originale, prima di inoltrare la richiesta alla risorsa protetta. Questa opzione è descritta nella sezione precedente,. Inserimenti personalizzati nell'intestazione della richiesta per azioni non bloccanti

Intestazioni di risposta personalizzate

È possibile specificare qualsiasi nome di intestazione ad eccezione di. `content-type`

Corpi di risposta personalizzati

Il corpo di una risposta personalizzata viene definito nel contesto dell'ACL Web o del gruppo di regole in cui si desidera utilizzarla. Dopo aver definito un corpo di risposta personalizzato, puoi utilizzarlo come riferimento in qualsiasi altro punto dell'ACL Web o del gruppo di regole in cui lo hai creato. Nelle impostazioni delle singole Block azioni, fai riferimento al corpo personalizzato che desideri utilizzare e definisci il codice di stato e l'intestazione della risposta personalizzata.

Quando crei una risposta personalizzata nella console, puoi scegliere tra i corpi di risposta che hai già definito oppure puoi creare un nuovo corpo. All'esterno della console, definisci i corpi di risposta personalizzati a livello di ACL Web o di gruppo di regole, quindi fai riferimento ad essi dalle impostazioni di azione all'interno dell'ACL Web o del gruppo di regole. Questo è illustrato nell'esempio JSON nella sezione seguente.

Esempio di risposta personalizzata

L'esempio seguente elenca il codice JSON per un gruppo di regole con impostazioni di risposta personalizzate. Il corpo della risposta personalizzato viene definito per l'intero gruppo di regole, quindi viene referenziato tramite chiave nell'azione della regola.

```
{
 "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
 }
}
```

Codici di stato supportati per una risposta personalizzata

Per informazioni dettagliate sui codici di stato HTTP, vedere Codici di stato dell'Internet Engineering Task Force (IETF) e Elenco dei codici di stato HTTP su Wikipedia.

Di seguito sono riportati i codici di stato HTTP che AWS WAF supportano le risposte personalizzate.

- 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 etichette sulle richieste web

Un'etichetta è costituita da metadati aggiunti a una richiesta Web mediante una regola corrispondente. Quando una regola corrisponde a una richiesta web, se la regola ha delle etichette specificate, le AWS WAF aggiunge alla richiesta. Le etichette rimangono disponibili sulla richiesta fino al termine della valutazione dell'ACL Web. È possibile accedere alle etichette nelle regole che verranno eseguite successivamente nella valutazione ACL Web utilizzando un'istruzione label match. Per informazioni dettagliate, vedi Dichiarazione della regola di corrispondenza delle etichette.

Le etichette sulle richieste Web generano i parametri delle CloudWatch etichette di Amazon. Per un elenco di metriche e dimensioni, consulta. Metriche e dimensioni delle etichette Per informazioni sull'accesso alle metriche e ai riepiloghi delle metriche tramite CloudWatch e attraverso la AWS WAF console, consulta. Monitoraggio e ottimizzazione

Casi d'uso dell'etichettatura

I casi d'uso più comuni per AWS WAF le etichette includono:

- Valutazione di una richiesta Web in base a più istruzioni di regole prima di intervenire sulla richiesta: dopo che viene trovata una corrispondenza con una regola in un ACL Web, AWS WAF continua a valutare la richiesta rispetto all'ACL Web se l'azione della regola non interrompe la valutazione dell'ACL Web. Puoi utilizzare le etichette per valutare e raccogliere informazioni

da più regole prima di decidere di consentire o bloccare la richiesta. A tale scopo, modifica le azioni relative alle regole esistenti Count e configurale per aggiungere etichette alle richieste corrispondenti. Quindi, aggiungi una o più nuove regole da eseguire dopo le altre regole e configurale per valutare le etichette e gestire le richieste in base alle combinazioni di corrispondenze delle etichette.

- Gestione delle richieste Web per area geografica: puoi utilizzare la sola regola di corrispondenza geografica per gestire le richieste Web in base al paese di origine. Per ottimizzare la posizione fino al livello della regione, si utilizza la regola di corrispondenza geografica con un'Countazione seguita da una regola di corrispondenza delle etichette. Per informazioni sulla regola del geo match, consulta. Istruzione regola di corrispondenza geografica
- Riutilizzo della logica su più regole: se è necessario riutilizzare la stessa logica su più regole, è possibile utilizzare le etichette come fonte unica della logica e verificare semplicemente i risultati. Quando sono presenti più regole complesse che utilizzano un sottoinsieme comune di istruzioni di regole annidate, la duplicazione del set di regole comuni tra le regole complesse può richiedere molto tempo e può essere soggetta a errori. Con le etichette, puoi creare una nuova regola con il sottoinsieme di regole comuni che conta le richieste corrispondenti e aggiunge loro un'etichetta. La nuova regola viene aggiunta all'ACL Web in modo che venga eseguita prima delle regole complesse originali. Quindi, nelle regole originali, sostituisci il sottoinsieme di regole condivise con un'unica regola che controlla l'etichetta.

  Ad esempio, supponiamo di avere più regole da applicare solo ai percorsi di accesso. Invece di fare in modo che ogni regola specifichi la stessa logica in base ai potenziali percorsi di accesso, puoi implementare un'unica nuova regola che contenga tale logica. Fai in modo che la nuova regola aggiunga un'etichetta alle richieste corrispondenti per indicare che la richiesta si trova su un percorso di accesso. Nell'ACL Web, assegna a questa nuova regola un'impostazione di priorità numerica inferiore rispetto alle regole originali in modo che venga eseguita per prima. Quindi, nelle regole originali, sostituisci la logica condivisa con un controllo della presenza dell'etichetta. Per informazioni sulle impostazioni di priorità, consultaOrdine di elaborazione delle regole e dei gruppi di regole in un ACL Web.
- Creazione di eccezioni alle regole nei gruppi di regole: questa opzione è particolarmente utile per i gruppi di regole gestiti, che non è possibile visualizzare o modificare. Molte regole gestite dei gruppi di regole aggiungono etichette alle richieste Web corrispondenti, per indicare le regole corrispondenti ed eventualmente per fornire informazioni aggiuntive sulla corrispondenza. Quando si utilizza un gruppo di regole che aggiunge etichette alle richieste, è possibile sovrascrivere le regole del gruppo di regole per contare le corrispondenze e quindi eseguire una regola dopo il gruppo di regole che gestisce la richiesta Web in base alle etichette del gruppo di regole. Tutte

le AWS Managed Rules aggiungono etichette alle richieste Web corrispondenti. Per i dettagli, consulta le descrizioni delle regole all'indirizzoAWS Elenco dei gruppi di regole di Managed Rules.

- Utilizzo delle metriche delle etichette per monitorare i modelli di traffico: puoi accedere alle metriche per le etichette che aggiungi tramite le tue regole e per le metriche aggiunte da qualsiasi gruppo di regole gestito utilizzato nell'ACL web. Tutti i gruppi di regole AWS Managed Rules aggiungono etichette alle richieste Web che valutano. Per un elenco delle metriche e delle dimensioni delle etichette, consultaMetriche e dimensioni delle etichette. Puoi accedere alle metriche e ai riepiloghi delle metriche tramite CloudWatch e tramite la pagina Web ACL nella console. AWS WAF Per informazioni, consulta Monitoraggio e ottimizzazione.

Come funziona l'etichettatura

Quando una regola corrisponde a una richiesta web, se la regola ha delle etichette definite, AWS WAF aggiunge le etichette alla richiesta al termine della valutazione della regola. Le regole che vengono valutate dopo la regola di corrispondenza nell'ACL Web possono corrispondere alle etichette aggiunte dalla regola.

Chi aggiunge etichette alle richieste

I componenti Web ACL che valutano le richieste possono aggiungere etichette alle richieste.

- Qualsiasi regola che non sia una dichiarazione di riferimento per un gruppo di regole può aggiungere etichette alle richieste Web corrispondenti. I criteri di etichettatura fanno parte della definizione della regola e, quando una richiesta Web corrisponde alla regola, AWS WAF aggiunge le etichette della regola alla richiesta. Per informazioni, consulta the section called “Aggiungere un'etichetta”.
- L'istruzione geo match rule aggiunge etichette di paesi e regioni a qualsiasi richiesta che esamina, indipendentemente dal fatto che l'istruzione produca una corrispondenza. Per informazioni, consulta the section called “Corrispondenza geografica”.
- Le regole AWS gestite per AWS WAF tutti aggiungono etichette alle richieste che esaminano. Aggiungono alcune etichette in base alle corrispondenze delle regole nel gruppo di regole e altre in base ai AWS processi utilizzati dai gruppi di regole gestiti, come l'etichettatura dei token aggiunta quando si utilizza un gruppo di regole di mitigazione intelligente delle minacce. Per informazioni sulle etichette aggiunte da ciascun gruppo di regole gestito, vedere. the section called “AWS Elenco dei gruppi di regole di Managed Rules”

Come AWS WAF gestisce le etichette

AWS WAF aggiunge le etichette della regola alla richiesta al termine dell'ispezione della richiesta da parte della regola. L'etichettatura fa parte delle attività di abbinamento di una regola, analogamente all'azione.

Le etichette non persistono nella richiesta Web dopo la fine della valutazione dell'ACL Web. Affinché altre regole corrispondano a un'etichetta aggiunta dalla regola, l'azione della regola non deve interrompere la valutazione della richiesta web da parte dell'ACL web. L'azione della regola deve essere impostata su CountCAPTCHA, o. Challenge Quando la valutazione dell'ACL Web non termina, le regole successive nell'ACL Web possono eseguire i criteri di corrispondenza delle etichette rispetto alla richiesta. Per ulteriori informazioni sulle operazioni delle regole, consulta Operazione delle regole.

Come accedere alle etichette durante la valutazione dell'ACL web

Una volta aggiunte, le etichette rimangono disponibili sulla richiesta fintanto che la richiesta AWS WAF viene valutata rispetto all'ACL web. Qualsiasi regola in un ACL Web può accedere alle etichette che sono state aggiunte dalle regole già eseguite nello stesso ACL Web. Ciò include le regole definite direttamente all'interno dell'ACL Web e le regole definite all'interno dei gruppi di regole utilizzati nell'ACL Web.

- È possibile eseguire il confronto con un'etichetta nei criteri di ispezione della richiesta della regola utilizzando l'istruzione label match. Puoi eseguire il confronto con qualsiasi etichetta allegata alla richiesta. Per i dettagli della dichiarazione, consultaDichiarazione della regola di corrispondenza delle etichette.
- L'istruzione Geographic Match aggiunge etichette con o senza corrispondenza, ma sono disponibili solo dopo che la regola ACL web contenente l'istruzione ha completato la valutazione della richiesta.
  - Non è possibile utilizzare una sola regola, ad esempio un'`AND`istruzione logica, per eseguire un'istruzione geo match seguita da un'istruzione label match rispetto alle etichette geografiche. È necessario inserire l'istruzione label match in una regola separata che segue la regola che contiene l'istruzione geo match.
  - Se si utilizza un'istruzione geo match come istruzione scope-down all'interno di un'istruzione di regola basata sulla frequenza o di un'istruzione di riferimento per un gruppo di regole gestito, le etichette aggiunte dall'istruzione geo match non possono essere esaminate dall'istruzione della regola che la contiene. Se è necessario controllare l'etichettatura geografica in un'istruzione di regole basata sulle tariffe o in un gruppo di regole, è necessario eseguire l'istruzione geo match in una regola separata che viene eseguita in precedenza.

Come accedere alle informazioni sulle etichette al di fuori della valutazione ACL Web

Le etichette non persistono nella richiesta Web al termine della valutazione dell'ACL Web, ma AWS WAF registrano le informazioni sulle etichette nei log e nelle metriche.

- AWS WAF memorizza i CloudWatch parametri di Amazon per le prime 100 etichette su ogni singola richiesta. Per informazioni sull'accesso ai parametri delle etichette, consulta Monitoraggio con Amazon CloudWatch e. Metriche e dimensioni delle etichette
- AWS WAF riassume le metriche delle CloudWatch etichette nei dashboard di panoramica del traffico Web ACL nella console. AWS WAF Puoi accedere ai dashboard da qualsiasi pagina Web ACL. Per ulteriori informazioni, consulta Dashboard di panoramica sul traffico ACL Web.
- AWS WAF registra le etichette nei registri per le prime 100 etichette su richiesta. È possibile utilizzare le etichette, insieme all'azione della regola, per filtrare i AWS WAF registri registrati. Per informazioni, consulta Registrazione del traffico AWS WAF ACL Web.

La tua valutazione ACL Web può applicare più di 100 etichette a una richiesta Web e confrontarle con più di 100 etichette, ma registra AWS WAF solo le prime 100 nei log e nelle metriche.

Requisiti per la sintassi e la denominazione delle etichette

Un'etichetta è una stringa composta da un prefisso, namespace opzionali e un nome. I componenti di un'etichetta sono delimitati da due punti. Le etichette hanno i seguenti requisiti e caratteristiche:

- Le etichette distinguono tra maiuscole e minuscole.
- Ogni spazio dei nomi o nome di etichetta può contenere fino a 128 caratteri.
- È possibile specificare fino a cinque namespace in un'etichetta.
- I componenti di un'etichetta sono separati da due punti (). `:`
- Non è possibile utilizzare le seguenti stringhe riservate nei namespace o nel nome specificati per un'etichetta:`awswaf`,,,,`aws`, `waf` `rulegroupwebacl`, `regexpatternset` e. `ipset` `managed`

Sintassi dell'etichetta

Un'etichetta completamente qualificata ha un prefisso, spazi dei nomi opzionali e un nome di etichetta. Il prefisso identifica il gruppo di regole o il contesto ACL web della regola che ha aggiunto l'etichetta. I namespace possono essere utilizzati per aggiungere ulteriore contesto all'etichetta. Il nome dell'etichetta fornisce il livello di dettaglio più basso per un'etichetta. Spesso indica la regola specifica che ha aggiunto l'etichetta alla richiesta.

Il prefisso dell'etichetta varia a seconda della sua origine.

- Le tue etichette: di seguito viene mostrata la sintassi completa delle etichette create nell'ACL Web e nelle regole del gruppo di regole. I tipi di entità sono `rulegroup` e. `webacl`

```
awswaf:<entity owner account id>:<entity type>:<entity name>:<custom
 namespace>:...:<label name>
```

  - Prefisso dello spazio dei nomi dell'etichetta: `awswaf:<entity owner account id>:<entity type>:<entity name>:`
  - Aggiunte di namespace personalizzati: `<custom namespace>:…:`

  Quando si definisce un'etichetta per una regola in un gruppo di regole o in un ACL Web, si controllano le stringhe dello spazio dei nomi personalizzate e il nome dell'etichetta. Il resto viene generato per te da. AWS WAF AWS WAF aggiunge automaticamente il prefisso a tutte le etichette `awswaf` e alle impostazioni dell'account e dell'ACL Web o dell'entità del gruppo di regole.

- Etichette dei gruppi di regole gestite: di seguito viene mostrata la sintassi completa delle etichette create dalle regole nei gruppi di regole gestiti.

```
awswaf:managed:<vendor>:<rule group name>:<custom namespace>:...:<label name>
```

  - Prefisso dello spazio dei nomi dell'etichetta: `awswaf:managed:<vendor>:<rule group name>:`
  - Aggiunte di namespace personalizzati: `<custom namespace>:…:`

  Tutti i gruppi di regole AWS Managed Rules aggiungono etichette. Per informazioni sui gruppi di regole gestite, consulta Gruppi di regole gestite.

- Etichette di altri AWS processi: questi processi vengono utilizzati dai gruppi di regole AWS Managed Rules, quindi vengono aggiunti alle richieste Web valutate utilizzando i gruppi di regole gestite. Di seguito viene illustrata la sintassi completa delle etichette per le etichette create dai processi richiamati dai gruppi di regole gestiti.

```
awswaf:managed:<process>:<custom namespace>:...:<label name>
```

  - Prefisso dello spazio dei nomi dell'etichetta: `awswaf:managed:<process>:`
  - Aggiunte di namespace personalizzati: `<custom namespace>:…:`

Le etichette di questo tipo sono elencate per i gruppi di regole gestiti che richiamano il processo. AWS Per informazioni sui gruppi di regole gestite, consulta Gruppi di regole gestite.

Esempi di etichette per le tue regole

Le seguenti etichette di esempio sono definite da regole in un gruppo di regole denominato `testRules` che appartiene all'account, 111122223333.

```
awswaf:111122223333:rulegroup:testRules:testNS1:testNS2:LabelNameA
```

```
awswaf:111122223333:rulegroup:testRules:testNS1:LabelNameQ
```

```
awswaf:111122223333:rulegroup:testRules:LabelNameZ
```

L'elenco seguente mostra un esempio di specifica di etichetta in JSON. Questi nomi di etichette includono stringhe di namespace personalizzate prima del nome dell'etichetta finale.

```
Rule: {
    Name: "label_rule",
    Statement: {...}
    RuleLabels: [
        Name: "header:encoding:utf8",
        Name: "header:user_agent:firefox"
    ],
    Action: { Count: {} }
}
```

> **Note**
>
> Puoi accedere a questo tipo di elenco nella console tramite l'editor di regole JSON.

Se si esegue la regola precedente nello stesso gruppo di regole e nello stesso account degli esempi di etichette precedenti, le etichette complete risultanti sarebbero le seguenti:

```
awswaf:111122223333:rulegroup:testRules:header:encoding:utf8
```

```
awswaf:111122223333:rulegroup:testRules:header:user_agent:firefox
```

Esempi di etichette per gruppi di regole gestiti

Di seguito sono riportati esempi di etichette provenienti dai gruppi di regole e dai processi di AWS Managed Rules da essi richiamati.

```
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
```

Aggiungere un'etichetta alle richieste web corrispondenti

Quando definisci un'etichetta per una regola, AWS WAF aggiunge l'etichetta alle richieste che corrispondono alla regola. Si definisce un'etichetta in una regola specificando le stringhe dello spazio dei nomi personalizzate e il nome da aggiungere al prefisso dello spazio dei nomi dell'etichetta. AWS WAF ricava il prefisso dal contesto in cui si definisce la regola. Per informazioni al riguardo, consulta le informazioni sulla sintassi dell'etichetta sotto. Requisiti per la sintassi e la denominazione delle etichette

Ad eccezione di quanto segue, puoi aggiungere etichette a qualsiasi regola e AWS WAF aggiungerai le tue etichette a qualsiasi richiesta web che corrisponda all'istruzione rule match:

- Le regole basate sulla frequenza aggiungono etichette alle richieste Web per l'istanza di aggregazione specifica solo quando tale istanza è limitata dalla frequenza. AWS WAF Per informazioni sulle regole basate sulla tariffa, consulta. Istruzione regola basata sulla frequenza
- Non è possibile utilizzare etichette nelle istruzioni che fanno riferimento a gruppi di regole. Se si tenta di aggiungere un'etichetta a un'istruzione di regole del gruppo di regole tramite l'API, l'operazione genera un'eccezione di convalida. Per informazioni su questi tipi di istruzioni, consulta Istruzione gruppo di regole gestite e. Istruzione gruppo di regole

WCU: 1 WCU ogni 5 etichette definite nelle regole dell'ACL Web o del gruppo di regole.

Dove trovarla

- Generatore di regole sulla console: nelle impostazioni di azione della regola, sotto Etichetta.
- Tipo di dati API: `Rule RuleLabels`

Corrispondenza a un'etichetta

Puoi utilizzare un'istruzione label match per valutare le etichette delle richieste web. È possibile eseguire il confronto con Label, che richiede il nome dell'etichetta, o con Namespace, che richiede una specifica dello spazio dei nomi. Per l'etichetta o lo spazio dei nomi, puoi facoltativamente includere gli spazi dei nomi precedenti e il prefisso nelle tue specifiche. Per informazioni generali su questo tipo di istruzione, vedere. Dichiarazione della regola di corrispondenza delle etichette

Il prefisso di un'etichetta definisce il contesto del gruppo di regole o dell'ACL web in cui viene definita la regola dell'etichetta. Nell'istruzione label match di una regola, se la stringa di corrispondenza dell'etichetta o dello spazio dei nomi non specifica il prefisso, AWS WAF utilizza il prefisso per la regola di corrispondenza dell'etichetta.

- Le etichette per le regole definite direttamente all'interno di un ACL Web hanno un prefisso che specifica il contesto ACL Web.
- Le etichette per le regole che si trovano all'interno di un gruppo di regole hanno un prefisso che specifica il contesto del gruppo di regole. Potrebbe trattarsi del tuo gruppo di regole o di un gruppo di regole gestito per te.

Per informazioni a riguardo, consulta la sintassi dell'etichetta sottoRequisiti per la sintassi e la denominazione delle etichette.

> **Note**
>
> Alcuni gruppi di regole gestiti aggiungono etichette. Puoi recuperarle tramite l'API `DescribeManagedRuleGroup` chiamando. Le etichette sono elencate nella `AvailableLabels` proprietà nella risposta.

Se desideri eseguire la corrispondenza con una regola che si trova in un contesto diverso da quello della tua regola, devi fornire il prefisso nella stringa di corrispondenza. Ad esempio, se desideri creare una corrispondenza con etichette aggiunte da regole in un gruppo di regole gestito, puoi aggiungere

una regola nell'ACL Web con un'istruzione label match la cui stringa di corrispondenza specifica il prefisso del gruppo di regole seguito dai criteri di corrispondenza aggiuntivi.

Nella stringa di corrispondenza per l'istruzione label match, specificate un'etichetta o uno spazio dei nomi:

- Etichetta: la specifica dell'etichetta per una corrispondenza è costituita dalla parte finale dell'etichetta. È possibile includere un numero qualsiasi di namespace contigui che precedono immediatamente il nome dell'etichetta seguito dal nome. È inoltre possibile fornire l'etichetta completamente qualificata avviando la specifica con il prefisso.

  Specifiche di esempio:

  - `testNS1:testNS2:LabelNameA`
  - `awswaf:managed:aws:managed-rule-set:testNS1:testNS2:LabelNameA`
- Namespace: la specifica dello spazio dei nomi per una corrispondenza è costituita da qualsiasi sottoinsieme contiguo della specifica dell'etichetta escluso il nome. È possibile includere il prefisso e includere una o più stringhe di namespace.

  Specifiche di esempio:

  - `testNS1:testNS2:`
  - `awswaf:managed:aws:managed-rule-set:testNS1:`

Esempi di abbinamenti tra etichette

Questa sezione fornisce esempi di specifiche di corrispondenza, per la dichiarazione della regola di corrispondenza delle etichette.

> **Note**
>
> Questi elenchi JSON sono stati creati nella console aggiungendo una regola a un ACL web con le specifiche label match, quindi modificando la regola e passando all'editor Rule JSON. Puoi anche ottenere il JSON per un gruppo di regole o un ACL web tramite le API o l'interfaccia a riga di comando.

Argomenti

- Corrispondenza a un'etichetta di un altro contesto
- Corrispondenza a un'etichetta di gruppo di regole gestite
- Confronta con uno spazio dei nomi locale
- Confronta con uno spazio dei nomi di un gruppo di regole gestito

Confronta con un'etichetta locale

Il seguente elenco JSON mostra un'istruzione label match per un'etichetta che è stata aggiunta localmente alla richiesta Web, nello stesso contesto di questa regola.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Se utilizzi questa dichiarazione di corrispondenza nell'account 111122223333, in una regola che definisci per l'ACL web`testWebACL`, corrisponderebbe alle seguenti etichette.

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

```
awswaf:111122223333:webacl:testWebACL:testNS1:testNS2:header:encoding:utf8
```

Non corrisponderebbe alla seguente etichetta, perché la stringa dell'etichetta non corrisponde esattamente.

```
awswaf:111122223333:webacl:testWebACL:header:encoding2:utf8
```

Non corrisponderebbe alla seguente etichetta, perché il contesto non è lo stesso, quindi il prefisso non corrisponde. Questo è vero anche se hai aggiunto il gruppo di regole `productionRules` all'ACL web`testWebACL`, dove è definita la regola.

```
awswaf:111122223333:rulegroup:productionRules:header:encoding:utf8
```

Corrispondenza a un'etichetta di un altro contesto

Il seguente elenco JSON mostra una regola di corrispondenza delle etichette che corrisponde a un'etichetta di una regola all'interno di un gruppo di regole creato dall'utente. Il prefisso è obbligatorio nelle specifiche per tutte le regole in esecuzione nell'ACL Web che non fanno parte del gruppo di regole denominato. Questo esempio di specifica dell'etichetta corrisponde solo all'etichetta esatta.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:111122223333:rulegroup:testRules:header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Corrispondenza a un'etichetta di gruppo di regole gestite

Si tratta di un caso speciale di abbinamento con un'etichetta proveniente da un contesto diverso da quello della regola di abbinamento. Il seguente elenco JSON mostra un'istruzione label match per un'etichetta di gruppo di regole gestita. Corrisponde solo all'etichetta esatta specificata nell'impostazione chiave dell'istruzione label match.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:managed:aws:managed-rule-set:header:encoding:utf8"
```

```
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Confronta con uno spazio dei nomi locale

Il seguente elenco JSON mostra un'istruzione label match per uno spazio dei nomi locale.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "NAMESPACE",
            Key: "header:encoding:"
        }
    },
    Labels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Analogamente alla `Label` corrispondenza locale, se si utilizza questa istruzione nell'account 111122223333, in una regola definita per l'ACL web`testWebACL`, corrisponderebbe alla seguente etichetta.

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

Non corrisponderebbe alla seguente etichetta, perché l'account non è lo stesso, quindi il prefisso non corrisponde.

```
awswaf:444455556666:webacl:testWebACL:header:encoding:utf8
```

Inoltre, il prefisso non corrisponde a nessuna etichetta applicata dai gruppi di regole gestiti, come la seguente.

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

Confronta con uno spazio dei nomi di un gruppo di regole gestito

Il seguente elenco JSON mostra un'istruzione label match per uno spazio dei nomi gestito per un gruppo di regole. Per un gruppo di regole di tua proprietà, devi anche fornire il prefisso per abbinarlo a uno spazio dei nomi che non rientra nel contesto della regola.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "NAMESPACE",
            Key: "awswaf:managed:aws:managed-rule-set:header:"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Questa specifica corrisponde alle seguenti etichette di esempio.

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

```
awswaf:managed:aws:managed-rule-set:header:encoding:unicode
```

Non corrisponde alla seguente etichetta.

```
awswaf:managed:aws:managed-rule-set:query:badstring
```

AWS WAF mitigazione intelligente delle minacce

Questa sezione illustra le funzionalità gestite di mitigazione intelligente delle minacce fornite da. AWS WAF Si tratta di protezioni avanzate e specializzate che puoi implementare per proteggerti da minacce come bot dannosi e tentativi di acquisizione di account.

> **Note**
>
> Le funzionalità qui descritte comportano costi aggiuntivi, oltre alle tariffe di base per l'utilizzo. AWS WAF Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

Le indicazioni fornite in questa sezione sono destinate agli utenti che conoscono in generale come creare e gestire ACL AWS WAF Web, regole e gruppi di regole. Questi argomenti sono trattati nelle sezioni precedenti di questa guida.

Argomenti

- Opzioni per la mitigazione intelligente delle minacce
- Le migliori pratiche per la mitigazione intelligente delle minacce
- AWS WAF token di richiesta web
- AWS WAF Fraud Control creazione di account e prevenzione delle frodi (ACFP)
- AWS WAF Controllo delle frodi e prevenzione delle acquisizioni di conti (ATP)
- AWS WAF Controllo dei bot
- AWS WAF integrazione delle applicazioni client
- CAPTCHAe Challenge in AWS WAF

Opzioni per la mitigazione intelligente delle minacce

Questa sezione fornisce un confronto dettagliato delle opzioni per l'implementazione della mitigazione intelligente delle minacce.

AWS WAF offre i seguenti tipi di protezioni per la mitigazione intelligente delle minacce.

- AWS WAF Fraud Control, creazione di account e prevenzione delle frodi (ACFP): rileva e gestisce i tentativi malevoli di creazione di account sulla pagina di registrazione dell'applicazione. La funzionalità principale è fornita dal gruppo di regole gestito ACFP. Per ulteriori informazioni, consultare AWS WAF Fraud Control creazione di account e prevenzione delle frodi (ACFP) e AWS WAF Gruppo di regole per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control.
- AWS WAF Fraud Control Account Takeover Prevention (ATP): rileva e gestisce i tentativi di acquisizione malevoli sulla pagina di accesso dell'applicazione. La funzionalità principale è fornita

dal gruppo di regole gestito dall'ATP. Per ulteriori informazioni, consultare AWS WAF Controllo delle frodi e prevenzione delle acquisizioni di conti (ATP) e AWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi.

- AWS WAF Bot Control: identifica, etichetta e gestisce bot amichevoli e dannosi. Questa funzionalità consente la gestione di bot comuni con firme uniche per tutte le applicazioni e anche di bot mirati con firme specifiche per un'applicazione. La funzionalità principale è fornita dal gruppo di regole gestito da Bot Control. Per ulteriori informazioni, consultare AWS WAF Controllo dei bot e AWS WAF Gruppo di regole Bot Control.
- SDK per l'integrazione delle applicazioni client: convalida le sessioni client e gli utenti finali sulle tue pagine Web e acquisisci AWS WAF token che i clienti possono utilizzare nelle loro richieste Web. Se utilizzi ACFP, ATP o Bot Control, implementa gli SDK di integrazione delle applicazioni nell'applicazione client, se possibile, per sfruttare appieno tutte le funzionalità del gruppo di regole. Consigliamo di utilizzare questi gruppi di regole senza un'integrazione SDK solo come misura temporanea, quando una risorsa critica deve essere protetta rapidamente e non c'è abbastanza tempo per l'integrazione con l'SDK. Per informazioni sull'implementazione degli SDK, consulta. AWS WAF integrazione delle applicazioni client
- Challengee azioni relative alle CAPTCHA regole: convalida le sessioni client e gli utenti finali e acquisisci AWS WAF token che i clienti possono utilizzare nelle loro richieste web. Puoi implementarli ovunque specifichi un'azione della regola, nelle tue regole e come sostituzioni nei gruppi di regole che utilizzi. Queste azioni utilizzano AWS WAF JavaScript interstitial per interrogare il client o l'utente finale e richiedono applicazioni client che supportino. JavaScript Per ulteriori informazioni, consulta CAPTCHAe Challenge in AWS WAF.

I gruppi di regole AWS Managed Rules per la mitigazione intelligente delle minacce ACFP, ATP e Bot Control utilizzano token per il rilevamento avanzato. Per informazioni sulle funzionalità abilitate dai token nei gruppi di regole, consulta, e. Perché dovresti usare gli SDK di integrazione delle applicazioni con ACFP Perché dovresti usare gli SDK di integrazione delle applicazioni con ATP Perché dovresti usare gli SDK di integrazione delle applicazioni con Bot Control

Le opzioni per implementare la mitigazione intelligente delle minacce vanno dall'uso di base delle azioni delle regole per eseguire sfide e imporre l'acquisizione di token, alle funzionalità avanzate offerte dai gruppi di regole AWS Managed Rules per la mitigazione intelligente delle minacce.

Le tabelle seguenti forniscono confronti dettagliati delle opzioni per le funzionalità di base e avanzate.

Argomenti

- Sfide e acquisizione di token

- Gruppi di regole gestiti per la mitigazione intelligente delle minacce
- Opzioni per la limitazione della velocità nelle regole basate sulla velocità e nelle regole mirate di Bot Control

Sfide e acquisizione di token

Puoi presentare sfide e acquisire token utilizzando gli SDK di integrazione delle AWS WAF applicazioni o le azioni delle regole e. Challenge CAPTCHA In generale, le azioni relative alle regole sono più facili da implementare, ma comportano costi aggiuntivi, interferiscono maggiormente con l'esperienza del cliente e richiedono. JavaScript Gli SDK richiedono la programmazione nelle applicazioni client, ma possono offrire un'esperienza cliente migliore, sono gratuiti e possono essere utilizzati con JavaScript o in applicazioni Android o iOS. Puoi utilizzare gli SDK di integrazione delle applicazioni solo con ACL Web che utilizzano uno dei gruppi di regole gestiti per la mitigazione intelligente delle minacce a pagamento, descritti nella sezione seguente.

Confronto tra le opzioni per le sfide e l'acquisizione di token

	Operazione delle regole Challenge	Operazione delle regole CAPTCHA	JavaScript Sfida SDK	Sfida SDK per dispositivi mobili
Di cosa si tratta	Regola l'azione che impone l'acquisizione del AWS WAF token presentando al client del browser una sfida silenziosa (interstitial)	Regola d'azione che impone l'acquisizione del AWS WAF token presentando all'utente finale del client una sfida visiva o audio (Interstitial)	Livello di integrazione delle applicazioni, per i browser client e altri dispositivi che eseguono. JavaScript Esegue il rendering della Silent Challenge e acquisisce un token	Livello di integrazione delle applicazioni, per applicazioni Android e iOS. Esegue il rendering nativo della Silent Challenge e acquisisce un token
Buona scelta per...	Convalida silenziosa rispetto alle	Convalida silenziosa e da parte dell'uten	Convalida silenziosa rispetto alle	Convalida silenziosa rispetto alle

	Operazione delle regole Challenge	Operazione delle regole CAPTCHA	JavaScript Sfida SDK	Sfida SDK per dispositivi mobili
	sessioni dei bot e imposizione dell'acquisizione di token per i clienti che supportano JavaScript	te finale rispetto alle sessioni di bot e imposizione dell'acquisizione di token, per i clienti che supportano JavaScript	sessioni di bot e imposizione dell'acquisizione di token per i clienti che supportano. JavaScript Gli SDK offrono la latenza più bassa e il miglior controllo sulla posizione in cui viene eseguito lo script di sfida nell'applicazione.	sessioni bot e imposizione dell'acquisizione di token per applicazioni mobili native su Android e iOS. Gli SDK offrono la latenza più bassa e il miglior controllo sulla posizione in cui viene eseguito lo script di sfida nell'applicazione.
Considerazioni sull'implementazione	Implementato come regola, impostazione delle azioni	Implementato come impostazione delle azioni di norma	Richiede uno dei gruppi di regole a pagamento ACFP, ATP o Bot Control nell'ACL web. Richiede la codifica nell'applicazione client.	Richiede uno dei gruppi di regole a pagamento ACFP, ATP o Bot Control nell'ACL Web. Richiede la codifica nell'applicazione client.

	Operazione delle regole Challenge	Operazione delle regole CAPTCHA	JavaScript Sfida SDK	Sfida SDK per dispositivi mobili
Considerazioni sul runtime	Flusso intrusivo per richieste senza token validi. Il cliente viene reindiriz zato a una AWS WAF sfida interstit ial. Aggiunge i round trip di rete e richiede una seconda valutazione della richiesta web.	Flusso intrusivo per richieste senza token validi. Il client viene reindiriz zato a un CAPTCHA interstitial AWS WAF . Aggiunge i round trip di rete e richiede una seconda valutazione della richiesta web.	Può essere eseguito dietro le quinte. Ti dà un maggiore controllo sull'esperienza della sfida.	Può essere eseguito dietro le quinte. Ti dà un maggiore controllo sull'esperienza della sfida.
Richiede JavaScript	Sì	Sì	Sì	No
Client supportati	Browser e dispositivi che eseguono Javascript	Browser e dispositivi che eseguono Javascript	Browser e dispositivi che eseguono Javascript	Dispositivi Android e iOS

	Operazione delle regole Challenge	Operazione delle regole CAPTCHA	JavaScript Sfida SDK	Sfida SDK per dispositivi mobili
Supporta applicazioni a pagina singola (SPA)	Solo esecuzione forzata. Puoi utilizzare l'Challengeazione insieme agli SDK per assicurarti che le richieste abbiano un token di sfida valido. Non puoi utilizzare l'azione della regola per inviare lo script di sfida alla pagina.	Solo applicazione. Puoi utilizzare l'CAPTCHAazione insieme agli SDK per assicurarti che le richieste abbiano un token CAPTCHA valido. Non puoi utilizzare l'azione della regola per inviare lo script CAPTCHA alla pagina.	Sì	N/D
Costo aggiuntivo	Sì, per le impostazioni delle azioni che specifichi esplicitamente, nelle regole che definisci o come regole che sostituiscono le azioni nei gruppi di regole che utilizzi. No in tutti gli altri casi.	Sì, per le impostazioni delle azioni che specifichi esplicitamente, nelle regole che definisci o come regole che sostituiscono le azioni nei gruppi di regole che utilizzi. No in tutti gli altri casi.	No, ma richiede uno dei gruppi di regole a pagamento ACFP, ATP o Bot Control.	No, ma richiede uno dei gruppi di regole a pagamento ACFP, ATP o Bot Control.

Per informazioni dettagliate sui costi associati a queste opzioni, consulta le informazioni sulla mitigazione intelligente delle minacce alla pagina Prezzi.AWS WAF

Può essere più semplice gestire le sfide e garantire l'applicazione di base dei token semplicemente aggiungendo una regola con un'azione Challenge oCAPTCHA. Potrebbe esserti richiesto di utilizzare le azioni della regola, ad esempio se non hai accesso al codice dell'applicazione.

Tuttavia, se riesci a implementare gli SDK, puoi risparmiare sui costi e ridurre la latenza nella valutazione ACL Web delle richieste Web dei client, rispetto all'utilizzo dell'azione: Challenge

- Puoi scrivere l'implementazione dell'SDK per eseguire la sfida in qualsiasi momento dell'applicazione. Puoi acquisire il token in background, prima di qualsiasi azione del cliente che invierebbe una richiesta web alla tua risorsa protetta. In questo modo, il token è disponibile per l'invio con la prima richiesta del cliente.
- Se invece acquisisci token implementando una regola con l'Challengeazione, la regola e l'azione richiedono un'ulteriore valutazione ed elaborazione della richiesta web quando il client invia una richiesta per la prima volta e ogni volta che il token scade. L'Challengeazione blocca la richiesta che non ha un token valido e non scaduto e invia la sfida interstitial al client. Dopo che il client ha risposto con successo alla sfida, l'interstitial invia nuovamente la richiesta web originale con il token valido, che viene quindi valutata una seconda volta dall'ACL web.

Gruppi di regole gestiti per la mitigazione intelligente delle minacce

I gruppi di regole AWS Managed Rules per la mitigazione intelligente delle minacce forniscono la gestione dei bot di base, il rilevamento e la mitigazione di bot sofisticati e dannosi, il rilevamento e la mitigazione dei tentativi di acquisizione degli account e il rilevamento e la mitigazione dei tentativi fraudolenti di creazione di account. Questi gruppi di regole, combinati con gli SDK per l'integrazione delle applicazioni descritti nella sezione precedente, forniscono le protezioni più avanzate e un accoppiamento sicuro con le applicazioni client.

Confronto tra le opzioni del gruppo di regole gestite

	ACFP	ATP	Livello comune di Bot Control	Bot Control: livello mirato
Che cos'è	Gestisce le richieste che potrebbero far parte di tentativi	Gestisce le richieste che potrebbero far parte di tentativi	Gestisce i bot comuni che si identific ano automatic	Gestisce bot mirati che non si identific ano automatic

	ACFP	ATP	Livello comune di Bot Control	Bot Control: livello mirato
	fraudolenti di creazione di account sulle pagine di registrazione e iscrizione di un'applicazione. Non gestisce i bot. Per informazioni, consulta AWS WAF Gruppo di regole per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control.	di acquisizione malevoli sulla pagina di accesso di un'applicazione. Non gestisce i bot. Per informazioni, consulta AWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi.	amente, con firme uniche per tutte le applicazioni. Per informazioni, consulta AWS WAF Gruppo di regole Bot Control.	amente, con firme specifiche per un'applicazione. Per informazioni, consulta AWS WAF Gruppo di regole Bot Control.

	ACFP	ATP	Livello comune di Bot Control	Bot Control: livello mirato
Buona scelta per...	Ispezione del traffico di creazione di account per individuare eventuali attacchi fraudolenti alla creazione di account, ad esempio tentativi di creazione con nome utente incrociato e creazione di molti nuovi account a partire da un unico indirizzo IP.	L'ispezione del traffico di accesso ai fini dell'acquisizione di account attacca, ad esempio, i tentativi di accesso con l'incrocio della password e molti tentativi di accesso dallo stesso indirizzo IP. Se utilizzato con i token, fornisce anche protezioni aggregate come la limitazione della velocità degli IP e delle sessioni client per volumi elevati di tentativi di accesso falliti.	Protezione dei bot di base ed etichettatura del traffico bot comune e automatizzato.	Protezione mirata contro bot sofisticati, inclusa la limitazione della velocità a livello di sessione del client e il rilevamento e la mitigazione degli strumenti di automazione del browser come Selenium e Puppeteer.
Aggiunge etichette che indicano i risultati della valutazione	Sì	Sì	Sì	Sì
Aggiunge etichette token	Sì	Sì	Sì	Sì

	ACFP	ATP	Livello comune di Bot Control	Bot Control: livello mirato
Blocco per le richieste che non hanno un token valido	Non incluso Per informazioni, consulta Bloccare le richieste che non hanno un token valido.	Non inclusa Per informazioni, consulta Bloccare le richieste che non hanno un token valido.	Non inclusa Per informazioni, consulta Bloccare le richieste che non hanno un token valido.	Blocca le sessioni client che inviano 5 richieste senza token.
Richiede il AWS WAF token `aws-waf-token`	Obbligatorio per tutte le regole. Per informazioni, consulta Perché dovresti usare gli SDK di integrazione delle applicazioni con ACFP.	Obbligatorio per molte regole. Per informazioni, consulta Perché dovresti usare gli SDK di integrazione delle applicazioni con ATP.	No	Sì
Acquisisce il token AWS WAF `aws-waf-token`	Sì, applicato secondo la regola `AllRequests`	No	No	Alcune regole utilizzano Challenge o CAPTCHA regolano azioni che acquisiscono token.

Per informazioni dettagliate sui costi associati a queste opzioni, consulta le informazioni sulla mitigazione intelligente delle minacce nella AWS WAF sezione Prezzi.

Opzioni per la limitazione della velocità nelle regole basate sulla velocità e nelle regole mirate di Bot Control

Il livello mirato del gruppo di regole AWS WAF Bot Control e l'istruzione della regola AWS WAF basata sulla frequenza forniscono entrambi la limitazione della frequenza delle richieste web. La tabella seguente confronta le due opzioni.

Confronto delle opzioni per il rilevamento e la mitigazione basati sulla frequenza

	AWS WAF regola basata sulla tariffa	AWS WAF Regole mirate di Bot Control	
Come viene applicata la limitazione della velocità	Agisce su gruppi di richieste che arrivano a una frequenza troppo elevata. È possibile applicare qualsiasi azione ad eccezione diAllow.	Applica modelli di accesso simili a quelli umani e applica una limitazione dinamica della velocità, tramite l'uso di token di richiesta.	
In base alle linee di base storiche del traffico?	No	Sì	
Tempo necessario per accumulare le linee di base storiche del traffico	N/D	Cinque minuti per le soglie dinamiche. N/A per token assente.	
Ritardo di mitigazione	Di solito 30-50 secondi. Può durare fino a diversi minuti.	Di solito meno di 10 secondi. Può durare fino a diversi minuti.	
Obiettivi di mitigazio ne	Configurabile. È possibile raggruppare le richieste utilizzando un'istruzione scope-down e in base a una o più chiavi di	Indirizzi IP e sessioni client	

	AWS WAF regola basata sulla tariffa	AWS WAF Regole mirate di Bot Control	
	aggregazione, ad esempio indirizzo IP, metodo HTTP e stringa di query.		
Livello di volume di traffico richiesto per attivare le mitigazioni	Medio: può contenere un minimo di 100 richieste nella finestra temporale specificata	Basso: destinato a rilevare i modelli ricorrenti dei client, ad esempio gli slow scraper	
Soglie personalizzabili	Sì	No	
Azione di mitigazione predefinita	L'impostazione predefinita della console èBlock. Nessuna impostazi one predefinita nell'API; l'imposta zione è obbligatoria. Puoi impostarla su qualsiasi azione di regola tranneAllow.	Le impostazioni di azione delle regole del gruppo di regole riguardano Challenge l'assenza di token e CAPTCHA il traffico ad alto volume proveniente da una singola sessione client. È possibile impostare una di queste regole su qualsiasi azione valida.	
Resilienza contro attacchi altamente distribuiti	Medio: massimo 10.000 indirizzi IP per la limitazione autonoma degli indirizzi IP	Medio: limitato a 50.000 in totale tra indirizzi IP e token	

	AWS WAF regola basata sulla tariffa	AWS WAF Regole mirate di Bot Control	
AWS WAF Prezzi	Incluso nelle tariffe standard per. AWS WAF	Incluso nelle tariffe per il livello mirato di mitigazione intellige nte delle minacce di Bot Control.	
Per ulteriori informazi oni	Istruzione regola basata sulla frequenza	AWS WAF Gruppo di regole Bot Control	

Le migliori pratiche per la mitigazione intelligente delle minacce

Segui le best practice riportate in questa sezione per l'implementazione più efficiente ed economica delle funzionalità intelligenti di mitigazione delle minacce.

- Implementa JavaScript gli SDK per l'integrazione delle applicazioni mobili: implementa l'integrazione delle applicazioni per abilitare l'intero set di funzionalità ACFP, ATP o Bot Control nel modo più efficace possibile. I gruppi di regole gestiti utilizzano i token forniti dagli SDK per separare il traffico client legittimo dal traffico indesiderato a livello di sessione. Gli SDK di integrazione delle applicazioni assicurano che questi token siano sempre disponibili. Per ulteriori dettagli, consultare la sezione seguente:
  - Perché dovresti usare gli SDK di integrazione delle applicazioni con ACFP
  - Perché dovresti usare gli SDK di integrazione delle applicazioni con ATP
  - Perché dovresti usare gli SDK di integrazione delle applicazioni con Bot Control

  Utilizza le integrazioni per implementare le sfide del tuo client e, per esempio JavaScript, per personalizzare il modo in cui i puzzle CAPTCHA vengono presentati agli utenti finali. Per informazioni dettagliate, vedi AWS WAF integrazione delle applicazioni client.

  Se personalizzi i puzzle CAPTCHA utilizzando l' JavaScript API e utilizzi l'azione della CAPTCHA regola in qualsiasi punto del tuo ACL web, segui le indicazioni per la gestione della risposta CAPTCHA nel tuo client all'indirizzo. AWS WAF Gestione di una risposta CAPTCHA da AWS WAF Questa guida si applica a tutte le regole che utilizzano l'CAPTCHAazione, incluse quelle del gruppo di regole gestito ACFP e il livello di protezione mirato del gruppo di regole gestito da Bot Control.

- Limita le richieste che invii ai gruppi di regole ACFP, ATP e Bot Control: dovrai sostenere costi aggiuntivi per l'utilizzo dei gruppi di regole Managed Rules per la mitigazione intelligente delle minacce. AWS Il gruppo di regole ACFP esamina le richieste agli endpoint di registrazione e creazione degli account specificati. Il gruppo di regole ATP esamina le richieste all'endpoint di accesso specificato. Il gruppo di regole Bot Control esamina ogni richiesta che lo raggiunge nella valutazione ACL web.

  Considerate i seguenti approcci per ridurre l'uso di questi gruppi di regole:

  - Escludi le richieste dall'ispezione con un'istruzione scope-down nell'istruzione del gruppo di regole gestito. È possibile eseguire questa operazione con qualsiasi istruzione nestable. Per informazioni, consulta Dichiarazioni delimitate.
  - Escludi le richieste dall'ispezione aggiungendo regole prima del gruppo di regole. Per le regole che non è possibile utilizzare in un'istruzione riportata verso il basso e per situazioni più complesse, come l'etichettatura seguita dalla corrispondenza delle etichette, è possibile aggiungere regole che precedono i gruppi di regole. Per informazioni, consulta Dichiarazioni delimitate e Nozioni di base sulla dichiarazione delle regole.
  - Esegui i gruppi di regole in base a regole meno costose. Se hai altre AWS WAF regole standard che bloccano le richieste per qualsiasi motivo, eseguile prima di questi gruppi di regole a pagamento. Per ulteriori informazioni sulle regole e sulla gestione delle regole, consultaNozioni di base sulla dichiarazione delle regole.
  - Se utilizzi più di uno dei gruppi di regole gestiti per la mitigazione intelligente delle minacce, eseguili nel seguente ordine per contenere i costi: Bot Control, ATP, ACFP.

  Per informazioni dettagliate sui prezzi, consulta Prezzi di AWS WAF.

- Abilita il livello di protezione mirato del gruppo di regole Bot Control durante il normale traffico web: alcune regole del livello di protezione mirato richiedono tempo per stabilire le linee di base per i normali schemi di traffico prima di poter riconoscere e rispondere a schemi di traffico irregolari o dannosi. Ad esempio, le `TGT_ML_*` regole richiedono fino a 24 ore per riscaldarsi.

  Aggiungi queste protezioni quando non subisci un attacco e concedi loro il tempo di stabilire le proprie linee di base prima di aspettarsi che rispondano in modo appropriato agli attacchi. Se si aggiungono queste regole durante un attacco, dopo che l'attacco si è placato, il tempo necessario per stabilire una linea di base è in genere dal doppio al triplo del tempo normalmente richiesto, a causa della distorsione causata dal traffico di attacco. Per ulteriori informazioni sulle regole e sugli eventuali tempi di riscaldamento richiesti, consulta. Elenco delle regole

- Per la protezione DDoS (Distributed Denial of Service), utilizza la mitigazione DDoS automatica a livello di applicazione Shield Advanced: i gruppi di regole di mitigazione intelligente delle minacce non forniscono protezione DDoS. ACFP protegge dai tentativi fraudolenti di creazione di account sulla pagina di registrazione dell'applicazione. L'ATP protegge dai tentativi di acquisizione dell'account sulla pagina di accesso. Bot Control si concentra sull'applicazione di modelli di accesso simili a quelli umani utilizzando token e limiti dinamici della velocità nelle sessioni client.

  Quando utilizzi Shield Advanced con la mitigazione automatica degli attacchi DDoS a livello di applicazione abilitata, Shield Advanced risponde automaticamente agli attacchi DDoS rilevati creando, valutando e implementando mitigazioni personalizzate per tuo conto. AWS WAF Per ulteriori informazioni su Shield Advanced, vedereAWS Shield Advanced panoramica, eAWS Shield Advanced protezioni a livello di applicazione (livello 7).
- Ottimizza e configura la gestione dei token: regola la gestione dei token dell'ACL Web per la migliore esperienza utente.
  - Per ridurre i costi operativi e migliorare l'esperienza dell'utente finale, ottimizza i tempi di immunità per la gestione dei token in modo che i requisiti di sicurezza lo consentano. Ciò riduce al minimo l'uso di puzzle CAPTCHA e sfide silenziose. Per informazioni, consulta Scadenza del timestamp: tempi di immunità dei token.
  - Per abilitare la condivisione dei token tra applicazioni protette, configura un elenco di domini token per il tuo ACL web. Per informazioni, consulta Domini token ed elenchi di domini.
- Rifiuta le richieste con specifiche arbitrarie dell'host: configura le risorse protette in modo che le `Host` intestazioni delle richieste Web corrispondano alla risorsa di destinazione. Puoi accettare un valore o un set specifico di valori, ad esempio `myExampleHost.com` e`www.myExampleHost.com`, ma non accettare valori arbitrari per l'host.
- Per gli Application Load Balancer che sono l'origine CloudFront delle distribuzioni, configurali CloudFront e AWS WAF per una corretta gestione dei token: se associ il tuo ACL Web a un Application Load Balancer e distribuisci Application Load Balancer come origine per una distribuzione, vedi. CloudFront Configurazione richiesta per gli Application Load Balancer che sono origini CloudFront
- Test e ottimizzazione prima della distribuzione: prima di implementare qualsiasi modifica all'ACL Web, segui le procedure di test e ottimizzazione riportate in questa guida per assicurarti di ottenere il comportamento previsto. Ciò è particolarmente importante per queste funzionalità a pagamento. Per indicazioni generali, vedereTest e ottimizzazione delle protezioni AWS WAF. Per informazioni specifiche sui gruppi di regole gestite a pagamento, consulta Test e implementazione di ACFPTest e implementazione dell'ATP, eTest e implementazione di AWS WAF Bot Control.

AWS WAF token di richiesta web

AWS WAF i token sono parte integrante delle protezioni avanzate offerte dalla mitigazione AWS WAF intelligente delle minacce. Un token, a volte chiamato impronta digitale, è una raccolta di informazioni su una singola sessione client che il client archivia e fornisce con ogni richiesta web. AWS WAF utilizza i token per identificare e separare le sessioni client dannose dalle sessioni legittime, anche quando entrambe provengono da un unico indirizzo IP. L'uso dei token impone costi trascurabili per gli utenti legittimi, ma costosi su larga scala per le botnet.

AWS WAF utilizza i token per supportare la funzionalità di sfida del browser e dell'utente finale, fornita dagli SDK di integrazione delle applicazioni e dalle regole action and. Challenge CAPTCHA Inoltre, i token abilitano le funzionalità del AWS WAF Bot Control e dei gruppi di regole gestiti per la prevenzione dell'acquisizione di account.

AWS WAF crea, aggiorna e crittografa i token per i clienti che rispondono con successo alle sfide silenziose e ai puzzle CAPTCHA. Quando un client con un token invia una richiesta web, include il token crittografato, lo AWS WAF decrittografa e ne verifica il contenuto.

Argomenti

Come AWS WAF utilizza i token

AWS WAF utilizza i token per registrare e verificare i seguenti tipi di convalida della sessione client:

- CAPTCHA — I puzzle CAPTCHA aiutano a distinguere i bot dagli utenti umani. Un CAPTCHA viene eseguito solo dall'azione della regola. CAPTCHA Una volta completato con successo il puzzle, lo script CAPTCHA aggiorna il timestamp CAPTCHA del token. Per ulteriori informazioni, consulta CAPTCHAe Challenge in AWS WAF.

- Sfida: le sfide vengono eseguite silenziosamente per aiutare a distinguere le sessioni regolari dei client dalle sessioni dei bot e per rendere più costoso il funzionamento dei bot. Quando la sfida viene completata con successo, lo script della sfida acquisisce automaticamente un nuovo token, AWS WAF se necessario, e quindi aggiorna il timestamp della sfida del token.

  AWS WAF esegue sfide nelle seguenti situazioni:

  - SDK di integrazione delle applicazioni: gli SDK di integrazione delle applicazioni vengono eseguiti all'interno delle sessioni dell'applicazione client e aiutano a garantire che i tentativi di accesso siano consentiti solo dopo che il client ha risposto con successo a una sfida. Per ulteriori informazioni, consulta AWS WAF integrazione delle applicazioni client.
  - Challengeazione delle regole: per ulteriori informazioni, vedere. CAPTCHAe Challenge in AWS WAF
  - CAPTCHA— Quando viene eseguito un codice CAPTCHA interstitial, se il client non ha ancora un token, lo script esegue prima automaticamente una sfida per verificare la sessione client e inizializzare il token.

I token sono richiesti da molte regole dei gruppi di regole Managed Rules per le minacce intelligenti. AWS Le regole utilizzano i token per fare cose come distinguere i client a livello di sessione, determinare le caratteristiche del browser e comprendere il livello di interattività umana sulla pagina Web dell'applicazione. Questi gruppi di regole richiamano la gestione dei AWS WAF token, che applica l'etichettatura dei token che i gruppi di regole poi controllano.

- AWS WAF Fraud Control, creazione di account e prevenzione delle frodi (ACFP): le regole ACFP richiedono richieste web con token validi. Per ulteriori informazioni sulle regole, consulta. AWS WAF Gruppo di regole per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control
- AWS WAF Fraud Control Account Takeover Prevention (ATP): le regole ATP che impediscono sessioni con i clienti ad alto volume e di lunga durata richiedono richieste web che abbiano un token valido con un timestamp della sfida non scaduto. Per ulteriori informazioni, consulta AWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi.
- AWS WAF Bot Control: le regole mirate di questo gruppo di regole impongono un limite al numero di richieste Web che un client può inviare senza un token valido e utilizzano il tracciamento delle sessioni di token per il monitoraggio e la gestione a livello di sessione. Se necessario, le regole applicano le azioni Challenge e CAPTCHA regolano l'acquisizione di token e un comportamento valido del client. Per ulteriori informazioni, consulta AWS WAF Gruppo di regole Bot Control.

Caratteristiche del token

Ogni token presenta le seguenti caratteristiche:

- Il token è memorizzato in un cookie denominato`aws-waf-token`.
- Il token è crittografato.
- Il token rileva le impronte digitali della sessione client con un identificatore granulare adesivo che contiene le seguenti informazioni:
  - Il timestamp dell'ultima risposta riuscita del cliente a una sfida silenziosa.
  - Il timestamp dell'ultima risposta riuscita dell'utente finale a un CAPTCHA. Questo è presente solo se utilizzi CAPTCHA nelle tue protezioni.
  - Informazioni aggiuntive sul comportamento dei clienti e dei clienti che possono aiutare a separare i clienti legittimi dal traffico indesiderato. Le informazioni includono vari identificatori e segnali lato client che possono essere utilizzati per rilevare attività automatizzate. Le informazioni raccolte non sono uniche e non possono essere associate a un singolo essere umano.
    - Tutti i token includono i dati delle interrogazioni del browser del client, come indicazioni di automazione e incongruenze nelle impostazioni del browser. Queste informazioni vengono recuperate dagli script eseguiti dall'Challengeazione e dagli SDK dell'applicazione client. Gli script interrogano attivamente il browser e inseriscono i risultati nel token.
    - Inoltre, quando si implementa un SDK per l'integrazione di applicazioni client, il token include informazioni raccolte passivamente sull'interattività dell'utente finale con la pagina dell'applicazione. L'interattività include i movimenti del mouse, la pressione dei tasti e le interazioni con qualsiasi modulo HTML presente nella pagina. Queste informazioni aiutano a AWS WAF rilevare il livello di interattività umana nel client, per sfidare utenti che non sembrano essere umani. Per informazioni sulle integrazioni lato client, consulta. AWS WAF integrazione delle applicazioni client

Per motivi di sicurezza, AWS non fornisce una descrizione completa del contenuto dei AWS WAF token o informazioni dettagliate sul processo di crittografia dei token.

Scadenza del timestamp: tempi di immunità dei token

AWS WAF utilizza i tempi di sfida e di immunità CAPTCHA per controllare la frequenza con cui una singola sessione client può essere sottoposta a una sfida o a un CAPTCHA. Dopo che un utente finale risponde con successo a un CAPTCHA, il tempo di immunità CAPTCHA determina per quanto tempo l'utente finale rimane immune dalla presentazione di un altro CAPTCHA. Allo stesso modo,

il tempo di immunità alla sfida determina per quanto tempo una sessione client rimane immune dall'essere nuovamente sfidata dopo aver risposto con successo a una sfida.

AWS WAF registra una risposta riuscita a una sfida o a un CAPTCHA aggiornando il timestamp corrispondente all'interno del token. Quando AWS WAF ispeziona il token per verificare la presenza di una sfida o di un CAPTCHA, sottrae il timestamp dall'ora corrente. Se il risultato è superiore al tempo di immunità configurato, il timestamp è scaduto.

È possibile configurare i tempi di sfida e immunità CAPTCHA nell'ACL Web e anche in qualsiasi regola che utilizza l'azione della regola or. CAPTCHA Challenge

- L'impostazione ACL Web predefinita per entrambi i tempi di immunità è di 300 secondi.
- È possibile specificare il tempo di immunità per qualsiasi regola che utilizza l'Challengeazione CAPTCHA o. Se non si specifica il tempo di immunità per la regola, questa eredita l'impostazione dall'ACL Web.
- Per una regola all'interno di un gruppo di regole che utilizza l'Challengeazione CAPTCHA o, se non si specifica il tempo di immunità per la regola, questa erediterà l'impostazione da ogni ACL Web in cui si utilizza il gruppo di regole.
- Gli SDK di integrazione delle applicazioni utilizzano il tempo di immunità alle sfide del Web ACL.

Il valore minimo per il tempo di immunità alla sfida è di 300 secondi. Il valore minimo per il tempo di immunità CAPTCHA è di 60 secondi. Il valore massimo per entrambi i tempi di immunità è 259.200 secondi o tre giorni.

Puoi utilizzare l'ACL Web e le impostazioni del tempo di immunità a livello di regola per ottimizzare l'CAPTCHAazione o il comportamento di gestione delle Challenge sfide dell'SDK. Ad esempio, potresti configurare regole che controllano l'accesso a dati altamente sensibili con tempi di immunità bassi e quindi impostare tempi di immunità più elevati nell'ACL web per consentire alle altre regole e agli SDK di ereditare.

In particolare, per quanto riguarda il CAPTCHA, la risoluzione di un enigma può peggiorare l'esperienza del cliente sul sito web, quindi ottimizzare il periodo di immunità CAPTCHA può aiutarvi a mitigare l'impatto sull'esperienza del cliente, pur continuando a fornire le protezioni desiderate.

Per ulteriori informazioni sulla regolazione dei tempi di immunità in base all'utilizzo delle azioni e delle regole, consulta. Challenge CAPTCHA Procedure consigliate per l'utilizzo Challenge delle azioni CAPTCHA e

Impostazione dei tempi di immunità dei token

Puoi impostare i tempi di immunità nell'ACL web e nelle regole che utilizzano le azioni e. Challenge CAPTCHA

Per informazioni generali sulla gestione di un ACL Web e delle relative regole, consulta. Utilizzo delle ACL Web

Dove impostare il tempo di immunità per un ACL web

- Console: quando modifichi l'ACL Web, nella scheda Regole, modifica e modifica le impostazioni nei riquadri di configurazione Web ACL CAPTCHA e Web ACL Challenge. Nella console, puoi configurare il web ACL CAPTCHA e sfidare i tempi di immunità solo dopo aver creato l'ACL web.
- Al di fuori della console: il tipo di dati Web ACL dispone di parametri di configurazione CAPTCHA e challenge, che puoi configurare e fornire per le operazioni di creazione e aggiornamento sull'ACL Web.

Dove impostare il tempo di immunità per una regola

- Console: quando si crea o si modifica una regola e si specifica l'Challengeazione CAPTCHA o, è possibile modificare l'impostazione del tempo di immunità della regola.
- Al di fuori della console: il tipo di dati della regola ha parametri di configurazione CAPTCHA e challenge, che puoi configurare quando definisci la regola.

Domini token ed elenchi di domini

Quando AWS WAF crea un token per un client, lo configura con un dominio di token. Quando AWS WAF ispeziona un token in una richiesta web, lo rifiuta come non valido se il relativo dominio non corrisponde a nessuno dei domini considerati validi per l'ACL web.

Per impostazione predefinita, accetta AWS WAF solo token la cui impostazione del dominio corrisponde esattamente al dominio host della risorsa associata all'ACL web. Questo è il valore dell'`Host`intestazione nella richiesta web. In un browser, puoi trovare questo dominio nella JavaScript `window.location.hostname` proprietà e nell'indirizzo che l'utente vede nella barra degli indirizzi.

È inoltre possibile specificare domini token accettabili nella configurazione ACL Web, come descritto nella sezione seguente. In questo caso, AWS WAF accetta sia le corrispondenze esatte con l'intestazione host sia le corrispondenze con i domini nell'elenco dei domini del token.

È possibile specificare i domini token AWS WAF da utilizzare durante l'impostazione del dominio e durante la valutazione di un token in un ACL Web. I domini specificati non possono essere suffissi pubblici come. `gov.au` Per i domini che non puoi usare, consulta l'elenco https://publicsuffix.org/list/public_suffix_list.dat in Elenco dei suffissi pubblici.

Configurazione dell'elenco dei domini del token ACL Web

Puoi configurare un ACL web per condividere i token su più risorse protette fornendo un elenco di domini token con i domini aggiuntivi che desideri accettare. AWS WAF Con un elenco di domini token, accetta AWS WAF comunque il dominio host della risorsa. Inoltre, accetta tutti i domini nell'elenco dei domini token, inclusi i sottodomini con prefisso.

Ad esempio, una specifica di dominio `example.com` nell'elenco dei domini token corrisponde a `example.com` (da`http://example.com/`)`api.example.com`, (da`http://api.example.com/`) e `www.example.com` (da). `http://www.example.com/` Non corrisponde a`example.api.com`, (da`http://example.api.com/`) o `apiexample.com` (da`http://apiexample.com/`).

Puoi configurare l'elenco dei domini dei token nell'ACL web quando lo crei o lo modifichi. Per informazioni generali sulla gestione di un ACL Web, consulta. Utilizzo delle ACL Web

Controllo dell'impostazione del dominio all'interno del token

AWS WAF crea token su richiesta degli script di sfida, che vengono eseguiti dagli SDK di integrazione delle applicazioni e dalle azioni delle regole Challenge andCAPTCHA.

Il dominio che AWS WAF imposta un token è determinato dal tipo di script di sfida che lo richiede e da qualsiasi configurazione aggiuntiva del dominio del token fornita dall'utente. AWS WAF imposta il dominio nel token sull'impostazione più breve e generale che può trovare nella configurazione.

- JavaScript SDK: puoi configurare l'JavaScript SDK con una specifica di dominio token, che può includere uno o più domini. I domini che configuri devono essere accettati, in base al dominio host protetto e all'elenco dei domini token dell'ACL Web. AWS WAF

  Quando AWS WAF emette un token per il client, imposta il dominio del token su uno che corrisponda al dominio host e sia il più breve, tra il dominio host e i domini nell'elenco configurato. Ad esempio, se il dominio host è `api.example.com` e l'elenco dei domini token ha`example.com`, viene AWS WAF utilizzato `example.com` nel token, perché corrisponde al dominio host ed è più breve. Se non fornisci un elenco di domini token nella configurazione dell' JavaScript API, AWS WAF imposta il dominio sul dominio host della risorsa protetta.

Per ulteriori informazioni, consulta Fornire domini da utilizzare nei token.

- Mobile SDK: nel codice dell'applicazione, devi configurare l'SDK mobile con una proprietà di dominio token. Questa proprietà deve essere un dominio che AWS WAF accetti, in base al dominio host protetto e all'elenco di domini token dell'ACL Web.

  Quando AWS WAF emette un token per il client, utilizza questa proprietà come dominio del token. AWS WAF non utilizza il dominio host nei token che emette per il client SDK mobile.

  Per ulteriori informazioni, consulta l'`WAFConfigurationdomainName`impostazione in. Le specifiche SDK AWS WAF per dispositivi mobili
- Challengeazione — Se specifichi un elenco di domini token nell'ACL Web, AWS WAF imposta il dominio del token su uno che corrisponda al dominio host e sia il più breve tra il dominio host e i domini nell'elenco. Ad esempio, se il dominio host è `api.example.com` e l'elenco dei domini token ha`example.com`, AWS WAF utilizza `example.com` nel token, perché corrisponde al dominio host ed è più breve. Se non fornisci un elenco di domini token nell'ACL web, AWS WAF imposta il dominio sul dominio host della risorsa protetta.

Etichettatura dei token da parte dei gruppi di regole gestiti per la mitigazione intelligente delle minacce

Questa sezione descrive le etichette che la gestione dei AWS WAF token aggiunge alle richieste web. Per informazioni sulle etichette, vedereAWS WAF etichette sulle richieste web.

Quando si utilizza uno qualsiasi dei gruppi di regole gestiti dai AWS WAF bot o dal controllo delle frodi, i gruppi di regole utilizzano la gestione dei AWS WAF token per ispezionare i token di richiesta Web e applicare l'etichettatura dei token alle richieste. Per informazioni sui gruppi di regole gestiti, consultaAWS WAF Gruppo di regole per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control, AWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi e. AWS WAF Gruppo di regole Bot Control

> **Note**
>
> AWS WAF applica le etichette dei token solo quando si utilizza uno di questi gruppi di regole gestite per la mitigazione intelligente delle minacce.

La gestione dei token può aggiungere le seguenti etichette alle richieste Web.

Etichetta della sessione del client

L'etichetta `awswaf:managed:token:id:`*`identifier`* contiene un identificatore univoco utilizzato dalla gestione dei AWS WAF token per identificare la sessione client. L'identificatore può cambiare se il client acquisisce un nuovo token, ad esempio dopo aver scartato il token che stava utilizzando.

> **Note**
>
> AWS WAF non riporta le CloudWatch metriche di Amazon per questa etichetta.

Etichette di stato dei token: etichetta i prefissi dello spazio dei nomi

Le etichette di stato dei token riportano lo stato del token e le informazioni sulla sfida e sul CAPTCHA in esso contenute.

Ogni etichetta di stato del token inizia con uno dei seguenti prefissi dello spazio dei nomi:

- `awswaf:managed:token:` — Utilizzata per riportare lo stato generale del token e per riportare lo stato delle informazioni sulla sfida del token.
- `awswaf:managed:captcha:` — Utilizzato per riportare lo stato delle informazioni CAPTCHA del token.

Etichette di stato dei token: nomi delle etichette

Dopo il prefisso, il resto dell'etichetta fornisce informazioni dettagliate sullo stato del token:

- `accepted` — Il token di richiesta è presente e contiene quanto segue:
  - Una sfida o una soluzione CAPTCHA valida.
  - Una sfida o un timestamp CAPTCHA non scaduti.
  - Una specifica di dominio valida per l'ACL web.

  Esempio: l'etichetta `awswaf:managed:token:accepted` indica che il token delle richieste Web ha una soluzione di sfida valida, un timestamp della sfida non scaduto e un dominio valido.
- `rejected` — Il token di richiesta è presente ma non soddisfa i criteri di accettazione.

  Oltre all'etichetta rifiutata, la gestione dei token aggiunge uno spazio dei nomi e un nome personalizzati per indicare il motivo.
  - `rejected:not_solved` — Al token manca la sfida o la soluzione CAPTCHA.

- `rejected:expired`— La sfida o il timestamp CAPTCHA del token sono scaduti, in base ai tempi di immunità del token configurati dall'ACL web.
- `rejected:domain_mismatch`— Il dominio del token non corrisponde alla configurazione del dominio token dell'ACL Web.
- `rejected:invalid`— non è AWS WAF riuscito a leggere il token indicato.

  Esempio: `awswaf:managed:captcha:rejected` le etichette `awswaf:managed:captcha:rejected:expired` indicano che la richiesta è stata rifiutata perché il timestamp CAPTCHA nel token ha superato il tempo di immunità del token CAPTCHA configurato nell'ACL web.

- `absent`— La richiesta non ha il token o il gestore del token non è riuscito a leggerlo.

  Esempio: l'etichetta `awswaf:managed:captcha:absent` indica che la richiesta non ha il token.

Bloccare le richieste che non hanno un token valido

Quando si utilizza la minaccia intelligente AWS Managed Rules`AWSManagedRulesACFPRuleSet`, i gruppi di regole e `AWSManagedRulesATPRuleSet`AWS`ManagedRulesBotControlRuleSet`, i gruppi di regole richiamano la gestione dei AWS WAF token per valutare lo stato del token di richiesta Web ed etichettare le richieste di conseguenza.

> **Note**
>
> L'etichettatura dei token viene applicata solo alle richieste Web valutate utilizzando uno di questi gruppi di regole gestiti.

Per informazioni sull'etichettatura applicata dalla gestione dei token, vedere la sezione precedente,. Etichettatura dei token da parte dei gruppi di regole gestiti per la mitigazione intelligente delle minacce

I gruppi di regole gestiti per la mitigazione intelligente delle minacce gestiscono quindi i requisiti dei token come segue:

- La `AWSManagedRulesACFPRuleSet` `AllRequests` regola è configurata per eseguire l'Challengeazione su tutte le richieste, bloccando efficacemente quelle che non hanno l'etichetta del `accepted` token.

- `AWSManagedRulesATPRuleSet`Blocca le richieste che hanno l'etichetta `rejected` token, ma non blocca le richieste con l'etichetta `absent` token.
- Il livello di protezione `AWSManagedRulesBotControlRuleSet` mirato rappresenta una sfida per i clienti dopo aver inviato cinque richieste senza un'etichetta `accepted` token. Non blocca una singola richiesta che non ha un token valido. Il livello di protezione comune del gruppo di regole non gestisce i requisiti dei token.

Per ulteriori dettagli sui gruppi di regole per le minacce intelligenti, consultaAWS WAF Gruppo di regole per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control, AWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi eAWS WAF Gruppo di regole Bot Control.

Per bloccare le richieste a cui mancano i token quando si utilizza il gruppo di regole gestito da Bot Control o ATP

Con i gruppi di regole Bot Control e ATP, è possibile che una richiesta senza un token valido esca dalla valutazione del gruppo di regole e continui a essere valutata dall'ACL web.

Per bloccare tutte le richieste a cui manca il relativo token o il cui token è stato rifiutato, aggiungi una regola da eseguire immediatamente dopo il gruppo di regole gestito per acquisire e bloccare le richieste che il gruppo di regole non gestisce per te.

Di seguito è riportato un esempio di elenco JSON per un ACL Web che utilizza il gruppo di regole gestito ATP. L'ACL web ha una regola aggiuntiva per acquisire l'`awswaf:managed:token:absent`etichetta e gestirla. La regola limita la valutazione alle richieste web che arrivano all'endpoint di accesso, in modo da corrispondere all'ambito del gruppo di regole ATP. La regola aggiunta è riportata in grassetto.

```
{
  "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:"
}
```

Configurazione richiesta per gli Application Load Balancer che sono origini CloudFront

Leggi questa sezione se associ il tuo ACL web a un Application Load Balancer e distribuisci Application Load Balancer come origine per una distribuzione. CloudFront

Con questa architettura, è necessario fornire la seguente configurazione aggiuntiva per gestire correttamente le informazioni sul token.

- CloudFront Configurare per inoltrare il `aws-waf-token` cookie all'Application Load Balancer. Per impostazione predefinita, CloudFront rimuove i cookie dalla richiesta Web prima di inoltrarla all'origine. Per mantenere il cookie token con la richiesta web, configura il comportamento CloudFront della cache in modo che includa solo il cookie token o tutti i cookie. Per informazioni su come eseguire questa operazione, consulta la sezione Memorizzazione nella cache dei contenuti basati sui cookie nella Amazon CloudFront Developer Guide.
- Configura AWS WAF in modo che riconosca il dominio della CloudFront distribuzione come dominio token valido. Per impostazione predefinita, CloudFront imposta l'`Host`intestazione sull'origine Application Load Balancer AWS WAF e la utilizza come dominio della risorsa protetta. Il browser client, tuttavia, vede la CloudFront distribuzione come dominio host e i token generati

per il client utilizzano il CloudFront dominio come dominio del token. Senza alcuna configurazione aggiuntiva, quando AWS WAF confronta il dominio di risorse protetto con il dominio token, si verificherà una mancata corrispondenza. Per risolvere questo problema, aggiungi il nome del dominio di CloudFront distribuzione all'elenco dei domini token nella configurazione ACL web. Per informazioni su come eseguire questa attività, consultare Configurazione dell'elenco dei domini del token ACL Web.

AWS WAF Fraud Control creazione di account e prevenzione delle frodi (ACFP)

La frode nella creazione di account è un'attività illegale online in cui un utente malintenzionato cerca di creare uno o più account falsi. Gli aggressori utilizzano account falsi per attività fraudolente come l'abuso di bonus promozionali e di iscrizione, l'impersonificazione di qualcuno e attacchi informatici come il phishing. La presenza di account falsi può avere un impatto negativo sulla vostra attività, danneggiando la vostra reputazione presso i clienti ed esponendovi a frodi finanziarie.

Puoi monitorare e controllare i tentativi di frode nella creazione di account implementando la funzione di prevenzione delle AWS WAF frodi nella creazione di account Fraud Control (ACFP). AWS WAF offre questa funzionalità nel gruppo di regole AWS Managed Rules `AWSManagedRulesACFPRuleSet` con SDK di integrazione delle applicazioni complementari.

Il gruppo di regole gestito ACFP etichetta e gestisce le richieste che potrebbero far parte di tentativi dannosi di creazione di account. Il gruppo di regole esegue questa operazione esaminando i tentativi di creazione di account che i client inviano all'endpoint di registrazione dell'account dell'applicazione.

ACFP protegge le pagine di registrazione dell'account monitorando le richieste di iscrizione all'account per rilevare eventuali attività anomale e bloccando automaticamente le richieste sospette. Il gruppo di regole utilizza identificatori di richiesta, analisi comportamentale e apprendimento automatico per rilevare le richieste fraudolente.

- Richiedi un'ispezione: ACFP ti offre visibilità e controllo sui tentativi anomali di creazione di account e sui tentativi che utilizzano credenziali rubate, per prevenire la creazione di account fraudolenti. ACFP controlla le combinazioni di e-mail e password confrontandole con il suo database di credenziali rubate, che viene aggiornato regolarmente man mano che nuove credenziali trapelate vengono trovate sul dark web. ACFP valuta i domini utilizzati negli indirizzi e-mail e monitora l'uso dei numeri di telefono e dei campi degli indirizzi per verificare le immissioni e rilevare comportamenti fraudolenti. ACFP aggrega i dati per indirizzo IP e sessione client, per rilevare e bloccare i client che inviano troppe richieste di natura sospetta.

- Ispezione delle risposte: per CloudFront le distribuzioni, oltre a controllare le richieste di creazione di account in entrata, il gruppo di regole ACFP controlla le risposte dell'applicazione ai tentativi di creazione di account, per tenere traccia delle percentuali di successo e fallimento. Utilizzando queste informazioni, ACFP può bloccare temporaneamente le sessioni client o gli indirizzi IP con troppi tentativi falliti. AWS WAF esegue l'ispezione della risposta in modo asincrono, in modo da non aumentare la latenza del traffico web.

> **Note**
>
> Quando utilizzi questo gruppo di regole gestito, ti vengono addebitati costi aggiuntivi. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

> **Note**
>
> La funzionalità ACFP non è disponibile per i pool di utenti di Amazon Cognito.

Argomenti

Componenti ACFP

I componenti principali della prevenzione delle AWS WAF frodi (ACFP) per la creazione di account Fraud Control sono i seguenti:

- **`AWSManagedRulesACFPRuleSet`**— Le regole di questo gruppo di regole AWS Managed Rules rilevano, etichettano e gestiscono vari tipi di attività fraudolente di creazione di account. Il gruppo di regole controlla le richieste HTTP `GET` text/html che i client inviano all'endpoint di registrazione dell'account specificato e le richieste `POST` web che i client inviano all'endpoint di registrazione dell'account specificato. Per le CloudFront distribuzioni protette, il gruppo di regole controlla anche le risposte che la distribuzione invia alle richieste di creazione di account. Per un elenco delle

regole di questo gruppo di regole, vedi. AWS WAF Gruppo di regole per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control Includi questo gruppo di regole nell'ACL Web utilizzando una dichiarazione di riferimento del gruppo di regole gestito. Per informazioni sull'utilizzo di questo gruppo di regole, vedereAggiungere il gruppo di regole gestite ACFP all'ACL Web.

> **Note**
>
> Quando utilizzi questo gruppo di regole gestito, ti vengono addebitati costi aggiuntivi. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

- Dettagli sulle pagine di registrazione e creazione dell'account dell'applicazione: è necessario fornire informazioni sulle pagine di registrazione e creazione dell'account quando si aggiunge il gruppo di `AWSManagedRulesACFPRuleSet` regole all'ACL Web. Ciò consente al gruppo di regole di restringere l'ambito delle richieste esaminate e di convalidare correttamente le richieste web di creazione di account. La pagina di registrazione deve accettare richieste in formato `GET` text/html. Il percorso di creazione dell'account deve accettare `POST` le richieste. Il gruppo di regole ACFP funziona con nomi utente in formato e-mail. Per ulteriori informazioni, consulta Aggiungere il gruppo di regole gestite ACFP all'ACL Web.
- Per CloudFront le distribuzioni protette, dettagli su come l'applicazione risponde ai tentativi di creazione di account: fornisci dettagli sulle risposte dell'applicazione ai tentativi di creazione di account e il gruppo di regole ACFP tiene traccia e gestisce i tentativi di creazione di account in blocco da un singolo indirizzo IP o da una singola sessione client. Per informazioni sulla configurazione di questa opzione, vedere. Aggiungere il gruppo di regole gestite ACFP all'ACL Web
- JavaScript e SDK per l'integrazione di applicazioni mobili: implementa gli AWS WAF JavaScript SDK per dispositivi mobili con la tua implementazione ACFP per abilitare l'intero set di funzionalità offerto dal gruppo di regole. Molte delle regole ACFP utilizzano le informazioni fornite dagli SDK per la verifica del client a livello di sessione e l'aggregazione del comportamento, necessarie per separare il traffico client legittimo dal traffico dei bot. Per ulteriori informazioni sugli SDK, consulta AWS WAF integrazione delle applicazioni client.

Puoi combinare la tua implementazione ACFP con quanto segue per aiutarti a monitorare, ottimizzare e personalizzare le tue protezioni.

- Registrazione e metriche: puoi monitorare il traffico e capire in che modo il gruppo di regole gestite ACFP lo influenza, configurando e abilitando i log e i parametri Amazon CloudWatch per il tuo ACL

web. Le etichette che vengono `AWSManagedRulesACFPRuleSet` aggiunte alle tue richieste Web sono incluse nei log e nelle CloudWatch metriche di Amazon. Per informazioni sulla registrazione e sulle metriche, consulta e. Registrazione del traffico AWS WAF ACL Web Monitoraggio con Amazon CloudWatch

A seconda delle esigenze e del traffico registrato, potresti voler personalizzare `AWSManagedRulesACFPRuleSet` l'implementazione. Ad esempio, potresti voler escludere parte del traffico dalla valutazione ACFP o modificare il modo in cui gestisce alcuni dei tentativi di frode alla creazione di account che identifica, utilizzando AWS WAF funzionalità come le dichiarazioni mirate o le regole di abbinamento delle etichette.

- Etichette e regole di abbinamento delle etichette: per tutte le regole incluse`AWSManagedRulesACFPRuleSet`, puoi impostare il comportamento di blocco in base al conteggio e quindi confrontarle con le etichette aggiunte dalle regole. Utilizza questo approccio per personalizzare il modo in cui gestisci le richieste Web identificate dal gruppo di regole gestito ACFP. Per ulteriori informazioni sull'etichettatura e sull'utilizzo delle istruzioni label match, consulta e. Dichiarazione della regola di corrispondenza delle etichette AWS WAF etichette sulle richieste web
- Richieste e risposte personalizzate: puoi aggiungere intestazioni personalizzate alle richieste consentite e inviare risposte personalizzate per le richieste che blocchi. Per fare ciò, abbini l'etichetta alle funzionalità AWS WAF personalizzate di richiesta e risposta. Per ulteriori informazioni sulla personalizzazione delle richieste e delle risposte, consultaRichieste e risposte web personalizzate in AWS WAF.

Perché dovresti usare gli SDK di integrazione delle applicazioni con ACFP

Consigliamo vivamente di implementare gli SDK di integrazione delle applicazioni, per un uso più efficiente del gruppo di regole ACFP.

- Funzionalità completa del gruppo di regole: la regola ACFP funziona `SignalClientInteractivityAbsentLow` solo con i token popolati dalle integrazioni dell'applicazione. Questa regola rileva e gestisce l'interattività umana anomala con la pagina dell'applicazione. Gli SDK di integrazione delle applicazioni sono in grado di rilevare la normale interattività umana tramite movimenti del mouse, pressioni di tasti e altre misurazioni. Gli interstitial inviati dalle regole agiscono CAPTCHA e non Challenge possono fornire questo tipo di dati.
- Latenza ridotta: la regola del gruppo di regole `AllRequests` applica l'azione della Challenge regola a qualsiasi richiesta che non abbia già un token di sfida. Quando ciò accade, la richiesta

viene valutata dal gruppo di regole due volte: una volta senza il token e poi una seconda volta dopo l'acquisizione del token tramite l'Challengeazione interstitial. Non ti viene addebitato alcun costo aggiuntivo per il solo utilizzo della `AllRequests` regola, ma questo approccio aumenta il sovraccarico del traffico web e aggiunge latenza all'esperienza dell'utente finale. Se acquisite il token lato client utilizzando le integrazioni dell'applicazione, prima di inviare la richiesta di creazione dell'account, il gruppo di regole ACFP valuta la richiesta una sola volta.

Per ulteriori informazioni sulle funzionalità dei gruppi di regole, vedere. AWS WAF Gruppo di regole per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control

Per informazioni sugli SDK, consultaAWS WAF integrazione delle applicazioni client. Per informazioni sui AWS WAF token, consulta. AWS WAF token di richiesta web Per informazioni sulle azioni delle regole, vedereCAPTCHAe Challenge in AWS WAF.

Aggiungere il gruppo di regole gestite ACFP all'ACL Web

Per configurare il gruppo di regole gestito ACFP in modo da riconoscere le attività fraudolente legate alla creazione di account nel traffico web, fornisci informazioni su come i clienti accedono alla tua pagina di registrazione e invii le richieste di creazione di account all'applicazione. Per CloudFront le distribuzioni Amazon protette, fornisci anche informazioni su come la tua applicazione risponde alle richieste di creazione di account. Questa configurazione si aggiunge alla normale configurazione per un gruppo di regole gestito.

Per la descrizione del gruppo di regole e l'elenco delle regole, vedereAWS WAF Gruppo di regole per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control.

> **Note**
>
> Il database delle credenziali rubate ACFP contiene solo nomi utente in formato e-mail.

Questa guida è destinata agli utenti che sanno in generale come creare e gestire ACL AWS WAF Web, regole e gruppi di regole. Questi argomenti sono trattati nelle sezioni precedenti di questa guida. Per informazioni di base su come aggiungere un gruppo di regole gestito all'ACL Web, consultaAggiungere un gruppo di regole gestito a un ACL Web tramite la console.

Segui le migliori pratiche

Utilizza il gruppo di regole ACFP in conformità con le migliori pratiche disponibili in. Le migliori pratiche per la mitigazione intelligente delle minacce

Per utilizzare il gruppo di **`AWSManagedRulesACFPRuleSet`** regole nell'ACL Web

1. Aggiungi il gruppo di regole AWS gestito `AWSManagedRulesACFPRuleSet` all'ACL web e modifica le impostazioni del gruppo di regole prima di salvare.

   > **Note**
   >
   > Quando utilizzi questo gruppo di regole gestito, ti vengono addebitati costi aggiuntivi. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

2. Nel riquadro di configurazione del gruppo di regole, fornisci le informazioni che il gruppo di regole ACFP utilizza per esaminare le richieste di creazione di account.

   a. Per Usa l'espressione regolare nei percorsi, attiva questa opzione se desideri eseguire la corrispondenza delle espressioni regolari AWS WAF per le specifiche del percorso della pagina di registrazione e creazione dell'account.

      AWS WAF supporta la sintassi del pattern utilizzata dalla libreria `libpcre` PCRE con alcune eccezioni. La libreria è documentata in PCRE - Perl Compatible Regular Expressions. Per informazioni sul AWS WAF supporto, vedere. Corrispondenza dei modelli di espressioni regolari in AWS WAF

   b. Per il percorso della pagina di registrazione, fornisci il percorso dell'endpoint della pagina di registrazione per la tua applicazione. Questa pagina deve accettare richieste in formato `GET` text/html. Il gruppo di regole esamina solo le richieste HTTP `GET` text/html verso l'endpoint della pagina di registrazione specificato.

      > **Note**
      >
      > La corrispondenza per gli endpoint non fa distinzione tra maiuscole e minuscole. Le specifiche Regex non devono contenere il flag`(?-i)`, che disabilita la corrispondenza senza distinzione tra maiuscole e minuscole. Le specifiche delle stringhe devono iniziare con una barra. `/`

Ad esempio, per l'URL`https://example.com/web/registration`, è possibile fornire la specifica `/web/registration` del percorso della stringa. I percorsi delle pagine di registrazione che iniziano con il percorso fornito vengono considerati corrispondenti. Ad esempio, `/web/registration` corrisponde ai percorsi di registrazione `/web/registration` `/web/registration//web/registrationPage`,, e`/web/registration/thisPage`, ma non corrisponde al percorso `/home/web/registration` o`/website/registration`.

> **Note**
>
> Assicurati che gli utenti finali carichino la pagina di registrazione prima di inviare una richiesta di creazione di account. Questo aiuta a garantire che le richieste di creazione dell'account inviate dal client includano token validi.

c. Per il percorso di creazione dell'account, fornisci l'URI nel tuo sito Web che accetta i nuovi dati utente completati. Questo URI deve accettare `POST` le richieste.

> **Note**
>
> La corrispondenza per gli endpoint non fa distinzione tra maiuscole e minuscole. Le specifiche Regex non devono contenere il flag`(?-i)`, che disabilita la corrispondenza senza distinzione tra maiuscole e minuscole. Le specifiche delle stringhe devono iniziare con una barra. `/`

Ad esempio, per l'URL`https://example.com/web/newaccount`, è possibile fornire la specifica `/web/newaccount` del percorso della stringa. I percorsi di creazione dell'account che iniziano con il percorso fornito sono considerati corrispondenti. Ad esempio, `/web/newaccount` corrisponde ai percorsi di creazione dell'account `/web/newaccount` `/web/newaccount//web/newaccountPage`,`/web/newaccount/thisPage`, e, ma non corrisponde al percorso `/home/web/newaccount` o`/website/newaccount`.

d. Per Request inspection, specifica in che modo l'applicazione accetta i tentativi di creazione dell'account fornendo il tipo di payload della richiesta e i nomi dei campi all'interno del corpo della richiesta in cui vengono forniti il nome utente, la password e altri dettagli per la creazione dell'account.

> **Note**
>
> Per i campi dell'indirizzo principale e del numero di telefono, fornisci i campi nell'ordine in cui appaiono nel payload della richiesta.

La specificazione dei nomi dei campi dipende dal tipo di payload.

- Tipo di payload JSON: specifica i nomi dei campi nella sintassi del puntatore JSON. Per informazioni sulla sintassi JSON Pointer, consultate la documentazione di Internet Engineering Task Force (IETF) Object Notation (JSON) Pointer. JavaScript

  Ad esempio, per l'esempio seguente JSON payload, la specifica del campo nome utente è `/signupform/username` e le specifiche del campo dell'indirizzo principale sono, e. `/signupform/addrp1` `/signupform/addrp2` `/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 di payload FORM_ENCODED: utilizza i nomi dei moduli HTML.

  Ad esempio, per un modulo HTML con elementi di immissione utente e password denominati `username1` e`password1`, la specifica del campo nome utente è `username1` e la specifica del campo password è. `password1`

e. Se stai proteggendo CloudFront le distribuzioni Amazon, sotto l'ispezione Response, specifica in che modo l'applicazione indica il successo o il fallimento nelle sue risposte ai tentativi di creazione di account.

> **Note**
>
> L'ispezione della risposta ACFP è disponibile solo negli ACL Web che proteggono le distribuzioni. CloudFront

Specificate un singolo componente nella risposta alla creazione dell'account che desiderate che ACFP controlli. Per i tipi di componenti Body e JSON, AWS WAF può ispezionare i primi 65.536 byte (64 KB) del componente.

Fornite i criteri di ispezione per il tipo di componente, come indicato dall'interfaccia. È necessario fornire i criteri di successo e di fallimento da ispezionare nel componente.

Ad esempio, supponiamo che l'applicazione indichi lo stato di un tentativo di creazione di un account nel codice di stato della risposta e lo utilizzi `200 OK` come esito positivo `401 Unauthorized` e/o `403 Forbidden` negativo. È necessario impostare il tipo di componente per l'ispezione della risposta su Codice di stato, quindi immettere nella casella di testo Operazione riuscita `200` e nella casella di testo Errore immettere `401` sulla prima riga e `403` sulla seconda.

Il gruppo di regole ACFP conta solo le risposte che soddisfano i criteri di ispezione con esito positivo o negativo. Le regole del gruppo di regole agiscono sui clienti quando hanno una percentuale di successo troppo alta tra le risposte conteggiate, al fine di mitigare i tentativi di creazione di account in massa. Per un comportamento accurato secondo le regole del gruppo di regole, assicurati di fornire informazioni complete sui tentativi di creazione di account riusciti e falliti.

Per vedere le regole che controllano le risposte relative alla creazione di account, cerca `VolumetricIPSuccessfulResponse` e `VolumetricSessionSuccessfulResponse` nell'elenco delle regole in[AWS WAF Gruppo di regole per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control](#).

3. Fornisci qualsiasi configurazione aggiuntiva che desideri per il gruppo di regole.

   È possibile limitare ulteriormente l'ambito delle richieste esaminate dal gruppo di regole aggiungendo un'istruzione scope-down all'istruzione del gruppo di regole gestito. Ad esempio, è possibile esaminare solo le richieste con un argomento di interrogazione o un cookie specifico. Il gruppo di regole esaminerà solo le richieste che corrispondono ai criteri dell'istruzione scope-

down e che vengono inviate ai percorsi di registrazione e creazione dell'account specificati nella configurazione del gruppo di regole. Per informazioni sulle istruzioni scope-down, vedere. Dichiarazioni delimitate

4. Salvate le modifiche nell'ACL Web.

Prima di implementare l'implementazione ACFP per il traffico di produzione, testala e ottimizzala in un ambiente di staging o test finché non ti senti a tuo agio con il potenziale impatto sul traffico. Quindi testa e ottimizza le regole in modalità di conteggio con il traffico di produzione prima di abilitarle. Per informazioni, consulta la sezione che segue.

Test e implementazione di ACFP

Questa sezione fornisce linee guida generali per la configurazione e il test di un'implementazione di prevenzione delle AWS WAF frodi (ACFP) per la creazione di account Fraud Control per il tuo sito. I passaggi specifici che scegli di seguire dipenderanno dalle tue esigenze, dalle risorse e dalle richieste web che ricevi.

Queste informazioni si aggiungono alle informazioni generali su test e ottimizzazione fornite all'indirizzoTest e ottimizzazione delle protezioni AWS WAF.

> **Note**
>
> AWS Le Managed Rules sono progettate per proteggerti dalle minacce web più comuni. Se utilizzati in conformità con la documentazione, i gruppi di regole AWS Managed Rules aggiungono un altro livello di sicurezza per le applicazioni. Tuttavia, i gruppi di regole AWS Managed Rules non sono intesi come sostituti delle responsabilità in materia di sicurezza, che sono determinate dalle AWS risorse selezionate. Fai riferimento al modello di responsabilità condivisa per assicurarti che le tue risorse AWS siano adeguatamente protette.

> **Rischio legato al traffico di produzione**
>
> Prima di implementare l'implementazione ACFP per il traffico di produzione, testala e ottimizzala in un ambiente di staging o di test finché non ti senti a tuo agio con il potenziale impatto sul traffico. Quindi testa e ottimizza le regole in modalità di conteggio con il traffico di produzione prima di abilitarle.

AWS WAF fornisce credenziali di test che è possibile utilizzare per verificare la configurazione ACFP. Nella procedura seguente, configurerai un ACL web di prova per utilizzare il gruppo di regole gestito ACFP, configurerai una regola per acquisire l'etichetta aggiunta dal gruppo di regole e quindi eseguirai un tentativo di creazione dell'account utilizzando queste credenziali di test. Verificherai che il tuo ACL web abbia gestito correttamente il tentativo controllando i CloudWatch parametri di Amazon per il tentativo di creazione dell'account.

Questa guida è destinata agli utenti che sanno in generale come creare e gestire ACL AWS WAF Web, regole e gruppi di regole. Questi argomenti sono trattati nelle sezioni precedenti di questa guida.

Per configurare e testare un'implementazione della prevenzione AWS WAF delle frodi (ACFP) per la creazione di un account Fraud Control

Esegui questi passaggi prima in un ambiente di test, poi in produzione.

1. Aggiungi il gruppo AWS WAF di regole gestito per la prevenzione delle frodi (ACFP) per la creazione di account di Fraud Control in modalità count

   > **Note**
   >
   > Ti vengono addebitati costi aggiuntivi quando utilizzi questo gruppo di regole gestito. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

   Aggiungi il gruppo di regole AWS Managed Rules `AWSManagedRulesACFPRuleSet` a un ACL web nuovo o esistente e configuralo in modo che non alteri il comportamento corrente dell'ACL web. Per informazioni dettagliate sulle regole e le etichette per questo gruppo di regole, consulta. AWS WAF Gruppo di regole per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control

   - Quando aggiungi il gruppo di regole gestito, modificalo e procedi come segue:
     - Nel riquadro di configurazione del gruppo di regole, fornisci i dettagli delle pagine di registrazione e creazione dell'account dell'applicazione. Il gruppo di regole ACFP utilizza queste informazioni per monitorare le attività di accesso. Per ulteriori informazioni, consulta Aggiungere il gruppo di regole gestite ACFP all'ACL Web.
     - Nel riquadro Regole, apri il menu a discesa Sostituisci tutte le azioni delle regole e scegli. Count Con questa configurazione, AWS WAF valuta le richieste in base a tutte le regole del

gruppo di regole e conta solo le corrispondenze risultanti, pur continuando ad aggiungere etichette alle richieste. Per ulteriori informazioni, consulta Sovrascrivere le azioni delle regole in un gruppo di regole.

Con questo override, è possibile monitorare il potenziale impatto delle regole gestite ACFP per determinare se aggiungere eccezioni, ad esempio eccezioni per casi d'uso interni.

- Posiziona il gruppo di regole in modo che venga valutato in base alle regole esistenti nell'ACL Web, con un'impostazione di priorità numericamente superiore a qualsiasi regola o gruppo di regole che stai già utilizzando. Per ulteriori informazioni, consulta Ordine di elaborazione delle regole e dei gruppi di regole in un ACL Web.

  In questo modo, la tua attuale gestione del traffico non viene interrotta. Ad esempio, se hai regole che rilevano il traffico dannoso come SQL injection o cross-site scripting, continueranno a rilevarlo e registrarlo. In alternativa, se disponi di regole che consentono il traffico noto e non dannoso, queste possono continuare a consentire tale traffico senza che venga bloccato dal gruppo di regole gestito ACFP. Potresti decidere di modificare l'ordine di elaborazione durante le attività di test e ottimizzazione.

2. Implementa gli SDK di integrazione delle applicazioni

Integra l' AWS WAF JavaScript SDK nei percorsi di registrazione e creazione dell'account del browser. AWS WAF fornisce anche SDK mobili per integrare dispositivi iOS e Android. Per ulteriori informazioni sugli SDK di integrazione, consulta. AWS WAF integrazione delle applicazioni client Per informazioni su questa raccomandazione, consultaPerché dovresti usare gli SDK di integrazione delle applicazioni con ACFP.

> **Note**
>
> Se non riesci a utilizzare gli SDK per l'integrazione delle applicazioni, puoi testare il gruppo di regole ACFP modificandolo nell'ACL Web e rimuovendo l'override che hai inserito nella regola. `AllRequests` Ciò abilita l'impostazione delle Challenge azioni della regola, per garantire che le richieste includano un token di sfida valido.
> Eseguite questa operazione prima in un ambiente di test e poi con grande attenzione nell'ambiente di produzione. Questo approccio ha il potenziale di bloccare gli utenti. Ad esempio, se il percorso della pagina di registrazione non accetta richieste `GET` text/html, questa configurazione delle regole può bloccare efficacemente tutte le richieste nella pagina di registrazione.

3. Abilita il campionamento, la registrazione e le metriche per l'ACL web

   Se necessario, configura la registrazione per l'ACL Web e abilita il campionamento e i parametri Amazon. CloudWatch Puoi utilizzare questi strumenti di visibilità per monitorare l'interazione del gruppo di regole gestito ACFP con il tuo traffico.

   - Per informazioni sulla configurazione e l'utilizzo della registrazione, vedere. Registrazione del traffico AWS WAF ACL Web
   - Per informazioni sui CloudWatch parametri di Amazon, consultaMonitoraggio con Amazon CloudWatch.
   - Per informazioni sul campionamento delle richieste web, consulta. Visualizzazione di un esempio di richieste Web

4. Associare l'ACL Web a una risorsa

   Se l'ACL web non è già associato a una risorsa di test, associala. Per informazioni, consulta Associazione o dissociazione di un ACL Web con una risorsa AWS.

5. Monitora il traffico e la corrispondenza delle regole ACFP

   Assicurati che il traffico normale fluisca e che le regole del gruppo di regole gestite da ACFP aggiungano etichette alle richieste web corrispondenti. Puoi vedere le etichette nei log e vedere i parametri ACFP e delle etichette nei parametri di Amazon. CloudWatch Nei log, le regole che hai sostituito per conteggiare nel gruppo di regole vengono visualizzate nel comando `ruleGroupList` con `action` set to count e `overriddenAction` indicano l'azione della regola configurata che hai ignorato.

6. Verifica le funzionalità di controllo delle credenziali del gruppo di regole

   Esegui un tentativo di creazione di account utilizzando le credenziali di test compromised e verifica che il gruppo di regole corrisponda a tali credenziali come previsto.

   a. Accedi alla pagina di registrazione dell'account della risorsa protetta e prova ad aggiungere un nuovo account. Usa la seguente coppia AWS WAF di credenziali di test e inserisci un test qualsiasi

      - Utente: `WAF_TEST_CREDENTIAL@wafexample.com`
      - Password: `WAF_TEST_CREDENTIAL_PASSWORD`

Queste credenziali di test sono classificate come credenziali compromesse e il gruppo di regole gestite ACFP aggiungerà l'`awswaf:managed:aws:acfp:signal:credential_compromised`etichetta alla richiesta di creazione dell'account, che puoi vedere nei log.

b. Nei registri ACL Web, cerca l'`awswaf:managed:aws:acfp:signal:credential_compromised`etichetta nel `labels` campo delle voci di registro per la richiesta di creazione dell'account di prova. Per ulteriori informazioni sulla registrazione, consulta Registrazione del traffico AWS WAF ACL Web.

Dopo aver verificato che il gruppo di regole acquisisca le credenziali compromesse come previsto, puoi adottare le misure necessarie per configurarne l'implementazione in base alle tue esigenze per la risorsa protetta.

7. Per le CloudFront distribuzioni, verifica la gestione da parte del gruppo di regole dei tentativi di creazione di account in blocco

   Esegui questo test per ogni criterio di risposta riuscita configurato per il gruppo di regole ACFP. Attendi almeno 30 minuti tra un test e l'altro.

   a. Per ogni criterio di successo, identifica nella risposta un tentativo di creazione di account che abbia successo in base a quel criterio di successo. Quindi, da una singola sessione client, esegui almeno 5 tentativi di creazione dell'account con successo in meno di 30 minuti. Un utente normalmente crea un solo account sul tuo sito.

      Dopo la creazione del primo account avvenuta con successo, la `VolumetricSessionSuccessfulResponse` regola dovrebbe iniziare a corrispondere alle altre risposte alla creazione dell'account, etichettandole e conteggiandole in base all'azione sostituita dalla regola. La regola potrebbe non rispondere alla prima o due a causa della latenza.

   b. Nei registri ACL Web, cerca l'`awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_` nel `labels` campo delle voci di registro per le richieste web di creazione dell'account di prova. Per ulteriori informazioni sulla registrazione, consulta Registrazione del traffico AWS WAF ACL Web.

Questi test verificano che i criteri di successo corrispondano alle risposte, verificando che i conteggi di successo aggregati dalla regola superino la soglia della regola. Dopo aver raggiunto la soglia, se continui a inviare richieste di creazione di account dalla stessa sessione, la regola continuerà a corrispondere finché la percentuale di successo non scenderà al di sotto della soglia. Anche se la soglia viene superata, la regola corrisponde ai tentativi di creazione dell'account riusciti o falliti dall'indirizzo di sessione.

8. Personalizza la gestione delle richieste web ACFP

   Se necessario, aggiungi le tue regole che consentono o bloccano esplicitamente le richieste, per modificare il modo in cui le regole ACFP le gestirebbero altrimenti.

   Ad esempio, puoi utilizzare le etichette ACFP per consentire o bloccare le richieste o per personalizzare la gestione delle richieste. È possibile aggiungere una regola di corrispondenza delle etichette dopo il gruppo di regole gestite ACFP per filtrare le richieste etichettate in base alla gestione che si desidera applicare. Dopo il test, mantieni le relative regole ACFP in modalità di conteggio e mantieni le decisioni sulla gestione delle richieste nella tua regola personalizzata. Per vedere un esempio, consulta Esempio ACFP: risposta personalizzata per credenziali compromesse.

9. Rimuovi le regole di test e abilita le impostazioni del gruppo di regole gestito ACFP

   A seconda della situazione, potresti aver deciso di lasciare alcune regole ACFP in modalità conteggio. Per le regole che desideri eseguire secondo la configurazione configurata all'interno del gruppo di regole, disabilita la modalità di conteggio nella configurazione del gruppo di regole ACL Web. Al termine del test, puoi anche rimuovere le regole di corrispondenza delle etichette di test.

10. Monitora e sintonizza

    Per assicurarti che le richieste web vengano gestite come desideri, monitora attentamente il traffico dopo aver abilitato la funzionalità ACFP che intendi utilizzare. Modificate il comportamento in base alle esigenze applicando le regole (rules count override) sul gruppo di regole e con le vostre regole.

Dopo aver terminato il test dell'implementazione del gruppo di regole ACFP, se non hai già integrato l' AWS WAF JavaScript SDK nelle pagine di registrazione e creazione dell'account del browser, ti consigliamo vivamente di farlo. AWS WAF fornisce anche SDK mobili per integrare dispositivi iOS e Android. Per ulteriori informazioni sugli SDK di integrazione, consulta. AWS WAF integrazione delle

applicazioni client Per informazioni su questa raccomandazione, consultaPerché dovresti usare gli SDK di integrazione delle applicazioni con ACFP.

AWS WAF Esempi di prevenzione delle frodi (ACFP) per la creazione di account Fraud Control

Questa sezione mostra configurazioni di esempio che soddisfano i casi d'uso comuni per le implementazioni di prevenzione delle AWS WAF frodi (ACFP) per la creazione di account Fraud Control.

Ogni esempio fornisce una descrizione del caso d'uso e quindi mostra la soluzione negli elenchi JSON per le regole configurate personalizzate.

> **Note**
>
> È possibile recuperare elenchi JSON come quelli mostrati in questi esempi tramite il download web di ACL JSON della console o l'editor JSON delle regole, oppure tramite l'`getWebACL`operazione nelle API e nell'interfaccia a riga di comando.

Argomenti

- Esempio ACFP: configurazione semplice
- Esempio ACFP: risposta personalizzata per credenziali compromesse
- Esempio ACFP: configurazione dell'ispezione della risposta

Esempio ACFP: configurazione semplice

Il seguente elenco JSON mostra un esempio di ACL web con un gruppo di regole gestito per la prevenzione delle AWS WAF frodi per la creazione di account Fraud Control (ACFP). Prendi nota delle configurazioni aggiuntive `CreationPath` e `RegistrationPagePath` delle configurazioni, oltre al tipo di payload e alle informazioni necessarie per individuare nuove informazioni sull'account nel payload, per verificarlo. Il gruppo di regole utilizza queste informazioni per monitorare e gestire le richieste di creazione di account. Questo codice JSON include le impostazioni generate automaticamente dall'ACL Web, come lo spazio dei nomi delle etichette e l'URL di integrazione dell'applicazione dell'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:"
}
```

Esempio ACFP: risposta personalizzata per credenziali compromesse

Per impostazione predefinita, il controllo delle credenziali eseguito dal gruppo di regole `AWSManagedRulesACFPRuleSet` gestisce le credenziali compromesse etichettando la richiesta e bloccandola. Per informazioni dettagliate sul gruppo di regole e sul comportamento delle regole, consulta. AWS WAF Gruppo di regole per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control

Per informare l'utente che le credenziali dell'account che ha fornito sono state compromesse, puoi fare quanto segue:

- Sostituisci la **`SignalCredentialCompromised`** regola con Count: in questo modo la regola conta ed etichetta solo le richieste corrispondenti.
- Aggiungi una regola di corrispondenza delle etichette con gestione personalizzata: configura questa regola in modo che corrisponda all'etichetta ACFP e per eseguire la gestione personalizzata.

I seguenti elenchi ACL Web mostrano il gruppo di regole gestite ACFP dell'esempio precedente, con l'azione della `SignalCredentialCompromised` regola sostituita dal conteggio. Con questa configurazione, quando questo gruppo di regole valuta una richiesta Web che utilizza credenziali compromesse, etichetterà la richiesta, ma non la bloccherà.

Inoltre, l'ACL Web ora ha una risposta personalizzata denominata `aws-waf-credential-compromised` e una nuova regola denominata. `AccountSignupCompromisedCredentialsHandling` La priorità delle regole è un'impostazione numerica più elevata rispetto al gruppo di regole, quindi viene eseguita dopo il gruppo di regole nella valutazione ACL Web. La nuova regola corrisponde a qualsiasi richiesta con l'etichetta delle credenziali compromessa del gruppo di regole. Quando la regola trova una corrispondenza, applica l'Blockazione alla richiesta con il corpo della risposta personalizzato. Il corpo di risposta personalizzato fornisce informazioni all'utente finale che le sue credenziali sono state compromesse e propone un'azione da intraprendere.

```
{
  "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}"
    }
  }
}
```

Esempio ACFP: configurazione dell'ispezione della risposta

Il seguente elenco JSON mostra un esempio di ACL web con un gruppo di regole gestito per la creazione di account AWS WAF Fraud Control per la prevenzione delle frodi (ACFP) configurato per controllare le risposte di origine. Nota la configurazione dell'ispezione della risposta, che specifica i codici di esito positivo e dello stato della risposta. Puoi anche configurare le impostazioni di successo

e risposta in base alle corrispondenze JSON di header, body e body. Questo codice JSON include le impostazioni generate automaticamente dall'ACL Web, come lo spazio dei nomi delle etichette e l'URL di integrazione dell'applicazione dell'ACL Web.

> **Note**
>
> L'ispezione della risposta ATP è disponibile solo negli ACL Web che proteggono le distribuzioni. CloudFront

```
{
  "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 Controllo delle frodi e prevenzione delle acquisizioni di conti (ATP)

L'acquisizione di un account è un'attività illegale online in cui un utente malintenzionato ottiene l'accesso non autorizzato all'account di una persona. L'aggressore potrebbe farlo in diversi modi, ad esempio utilizzando credenziali rubate o indovinando la password della vittima attraverso una serie di tentativi. Quando l'aggressore ottiene l'accesso, potrebbe rubare denaro, informazioni o servizi alla vittima. L'aggressore potrebbe spacciarsi per vittima per accedere ad altri account di sua proprietà o per accedere agli account di altre persone o organizzazioni. Inoltre, potrebbero tentare di modificare la password dell'utente per bloccare la vittima dai propri account.

È possibile monitorare e controllare i tentativi di acquisizione dell'account implementando la funzione di prevenzione dell'acquisizione di account (ATP) di AWS WAF Fraud Control. AWS WAF offre questa funzionalità nel gruppo di regole AWS Managed Rules `AWSManagedRulesATPRuleSet` e negli SDK di integrazione delle applicazioni complementari.

Il gruppo di regole gestito da ATP etichetta e gestisce le richieste che potrebbero far parte di tentativi malevoli di acquisizione degli account. Il gruppo di regole esegue questa operazione esaminando i tentativi di accesso che i client inviano all'endpoint di accesso dell'applicazione.

- Richiedi un'ispezione: l'ATP ti offre visibilità e controllo sui tentativi di accesso anomali e sui tentativi di accesso che utilizzano credenziali rubate, per prevenire acquisizioni di account che potrebbero portare ad attività fraudolente. L'ATP verifica le combinazioni di e-mail e password confrontandole con il proprio database di credenziali rubate, che viene aggiornato regolarmente man mano che nuove credenziali trapelate vengono trovate sul dark web. L'ATP aggrega i dati in base all'indirizzo IP e alla sessione del client, per rilevare e bloccare i client che inviano troppe richieste di natura sospetta.
- Ispezione delle risposte: per CloudFront le distribuzioni, oltre a controllare le richieste di accesso in entrata, il gruppo di regole ATP controlla le risposte dell'applicazione ai tentativi di accesso, per tenere traccia delle percentuali di successo e di fallimento. Utilizzando queste informazioni, ATP può bloccare temporaneamente le sessioni client o gli indirizzi IP che presentano troppi errori di accesso. AWS WAF esegue l'ispezione della risposta in modo asincrono, in modo da non aumentare la latenza del traffico web.

> **Note**
>
> Quando utilizzi questo gruppo di regole gestito, ti vengono addebitati costi aggiuntivi. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

> **Note**
>
> La funzionalità ATP non è disponibile per i pool di utenti di Amazon Cognito.

Argomenti

Componenti ATP

I componenti principali della prevenzione dell'acquisizione di account (ATP) di AWS WAF Fraud Control sono i seguenti:

- **`AWSManagedRulesATPRuleSet`**— Le regole di questo gruppo di regole AWS Managed Rules rilevano, etichettano e gestiscono vari tipi di attività di acquisizione di account. Il gruppo di regole controlla le richieste `POST` web HTTP che i client inviano all'endpoint di accesso specificato. Per CloudFront le distribuzioni protette, il gruppo di regole controlla anche le risposte che la distribuzione invia a queste richieste. Per un elenco delle regole del gruppo di regole, vedere. AWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi Includi questo gruppo di regole nell'ACL Web utilizzando una dichiarazione di riferimento del gruppo di regole gestito. Per informazioni sull'utilizzo di questo gruppo di regole, vedereAggiungere il gruppo di regole gestite da ATP all'ACL Web.

  > **Note**
  >
  > Quando utilizzi questo gruppo di regole gestito, ti vengono addebitati costi aggiuntivi. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

- Dettagli sulla pagina di accesso dell'applicazione: è necessario fornire informazioni sulla pagina di accesso quando si aggiunge il gruppo di `AWSManagedRulesATPRuleSet` regole all'ACL Web. Ciò consente al gruppo di regole di restringere l'ambito delle richieste che esamina e di convalidare correttamente l'utilizzo delle credenziali nelle richieste Web. Il gruppo di regole ATP funziona con nomi utente in formato e-mail. Per ulteriori informazioni, consulta Aggiungere il gruppo di regole gestite da ATP all'ACL Web.
- Per CloudFront le distribuzioni protette, dettagli su come l'applicazione risponde ai tentativi di accesso: l'utente fornisce dettagli sulle risposte dell'applicazione ai tentativi di accesso e il gruppo di regole tiene traccia e gestisce i client che inviano troppi tentativi di accesso non riusciti. Per informazioni sulla configurazione di questa opzione, vedere. Aggiungere il gruppo di regole gestite da ATP all'ACL Web
- JavaScript e SDK per l'integrazione di applicazioni mobili: implementa gli AWS WAF JavaScript SDK per dispositivi mobili con la tua implementazione ATP per abilitare l'intero set di funzionalità offerto dal gruppo di regole. Molte regole ATP utilizzano le informazioni fornite dagli SDK per la verifica del client a livello di sessione e l'aggregazione del comportamento, necessarie per separare il traffico client legittimo dal traffico dei bot. Per ulteriori informazioni sugli SDK, consulta AWS WAF integrazione delle applicazioni client.

Puoi combinare la tua implementazione ATP con quanto segue per monitorare, ottimizzare e personalizzare le tue protezioni.

- Registrazione e metriche: puoi monitorare il traffico e capire in che modo il gruppo di regole gestite ATP lo influenza, configurando e abilitando i log e i CloudWatch parametri Amazon per il tuo ACL web. Le etichette che vengono `AWSManagedRulesATPRuleSet` aggiunte alle tue richieste Web sono incluse nei log e nelle CloudWatch metriche di Amazon. Per informazioni sulla registrazione e sulle metriche, consulta e. Registrazione del traffico AWS WAF ACL Web Monitoraggio con Amazon CloudWatch

  A seconda delle tue esigenze e del traffico registrato, potresti voler personalizzare `AWSManagedRulesATPRuleSet` l'implementazione. Ad esempio, potresti voler escludere parte del traffico dalla valutazione ATP o modificare il modo in cui gestisce alcuni dei tentativi di acquisizione dell'account che identifica, utilizzando AWS WAF funzionalità come le istruzioni riepilogative o le regole di abbinamento delle etichette.
- Etichette e regole di abbinamento delle etichette: per tutte le regole incluse`AWSManagedRulesATPRuleSet`, puoi impostare il comportamento di blocco in base al conteggio e quindi confrontarle con le etichette aggiunte dalle regole. Utilizzate questo approccio per personalizzare il modo in cui gestite le richieste Web identificate dal gruppo di regole gestito da ATP. Per ulteriori informazioni sull'etichettatura e sull'utilizzo delle istruzioni label match, consulta Dichiarazione della regola di corrispondenza delle etichette e. AWS WAF etichette sulle richieste web
- Richieste e risposte personalizzate: puoi aggiungere intestazioni personalizzate alle richieste consentite e inviare risposte personalizzate per le richieste che blocchi. Per fare ciò, abbini l'etichetta alle funzionalità AWS WAF personalizzate di richiesta e risposta. Per ulteriori informazioni sulla personalizzazione delle richieste e delle risposte, consultaRichieste e risposte web personalizzate in AWS WAF.

Perché dovresti usare gli SDK di integrazione delle applicazioni con ATP

Il gruppo di regole gestito da ATP richiede i token di sfida generati dagli SDK di integrazione delle applicazioni. I token abilitano l'intero set di protezioni offerto dal gruppo di regole.

Consigliamo vivamente di implementare gli SDK di integrazione delle applicazioni, per un uso più efficace del gruppo di regole ATP. Lo script di sfida deve essere eseguito prima del gruppo di regole ATP affinché il gruppo di regole possa beneficiare dei token acquisiti dallo script. Ciò avviene automaticamente con gli SDK di integrazione delle applicazioni. Se non riesci a utilizzare gli SDK,

puoi alternativamente configurare l'ACL web in modo che esegua l'azione Challenge o CAPTCHA regola tutte le richieste che verranno esaminate dal gruppo di regole ATP. L'utilizzo dell'azione Challenge o CAPTCHA rule può comportare costi aggiuntivi. Per i dettagli sui prezzi, vedere Prezzi di AWS WAF.

Funzionalità del gruppo di regole ATP che non richiedono un token

Quando le richieste web non dispongono di un token, il gruppo di regole gestito da ATP è in grado di bloccare i seguenti tipi di traffico:

- Indirizzi IP singoli che effettuano molte richieste di accesso.
- Indirizzi IP singoli che effettuano molte richieste di accesso non riuscite in un breve lasso di tempo.
- Tentativi di accesso con incrocio della password, utilizzando lo stesso nome utente ma cambiando la password.

Funzionalità del gruppo di regole ATP che richiedono un token

Le informazioni fornite nel token di sfida ampliano le funzionalità del gruppo di regole e della sicurezza complessiva delle applicazioni client.

Il token fornisce informazioni sul client con ogni richiesta web che consente al gruppo di regole ATP di separare le sessioni client legittime dalle sessioni client che si comportano male, anche se entrambe provengono da un unico indirizzo IP. Il gruppo di regole utilizza le informazioni contenute nei token per aggregare il comportamento delle richieste di sessione del client per un rilevamento e una mitigazione precisi.

Quando il token è disponibile nelle richieste Web, il gruppo di regole ATP può rilevare e bloccare le seguenti categorie aggiuntive di client a livello di sessione:

- Sessioni client che superano la sfida silenziosa gestita dagli SDK.
- Sessioni client che utilizzano nomi utente o password. Questa operazione è nota anche come credential stuffing.
- Sessioni client che utilizzano ripetutamente credenziali rubate per accedere.
- Sessioni client che impiegano molto tempo a cercare di accedere.
- Sessioni client che effettuano molte richieste di accesso. Il gruppo di regole ATP offre un migliore isolamento dei client rispetto alla regola AWS WAF basata sulla velocità, che può bloccare i client in base all'indirizzo IP. Il gruppo di regole ATP utilizza anche una soglia inferiore.

- Sessioni client che effettuano molte richieste di accesso non riuscite in un breve lasso di tempo. Questa funzionalità è disponibile per le CloudFront distribuzioni protette di Amazon.

Per ulteriori informazioni sulle funzionalità dei gruppi di regole, consultaAWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi.

Per informazioni sugli SDK, consultaAWS WAF integrazione delle applicazioni client. Per informazioni sui AWS WAF token, consulta. AWS WAF token di richiesta web Per informazioni sulle azioni delle regole, vedereCAPTCHAe Challenge in AWS WAF.

Aggiungere il gruppo di regole gestite da ATP all'ACL Web

Per configurare il gruppo di regole gestito da ATP in modo che riconosca le attività di acquisizione di account nel traffico web, fornisci informazioni su come i client inviano le richieste di accesso all'applicazione. Per CloudFront le distribuzioni protette di Amazon, fornisci anche informazioni su come l'applicazione risponde alle richieste di accesso. Questa configurazione si aggiunge alla normale configurazione per un gruppo di regole gestito.

Per la descrizione del gruppo di regole e l'elenco delle regole, vedereAWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi.

> **Note**
>
> Il database delle credenziali rubate ATP contiene solo nomi utente in formato e-mail.

Questa guida è destinata agli utenti che sanno in generale come creare e gestire ACL AWS WAF Web, regole e gruppi di regole. Questi argomenti sono trattati nelle sezioni precedenti di questa guida. Per informazioni di base su come aggiungere un gruppo di regole gestito all'ACL Web, consultaAggiungere un gruppo di regole gestito a un ACL Web tramite la console.

Segui le migliori pratiche

Utilizza il gruppo di regole ATP in conformità con le migliori pratiche riportate inLe migliori pratiche per la mitigazione intelligente delle minacce.

Per utilizzare il gruppo di **`AWSManagedRulesATPRuleSet`** regole nell'ACL Web

1. Aggiungi il gruppo di regole AWS gestito `AWSManagedRulesATPRuleSet` all'ACL web e modifica le impostazioni del gruppo di regole prima di salvare.

> **Note**
>
> Quando utilizzi questo gruppo di regole gestito, ti vengono addebitati costi aggiuntivi. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

2. Nel riquadro di configurazione del gruppo di regole, fornisci le informazioni che il gruppo di regole ATP utilizza per esaminare le richieste di accesso.

   a. Per Usa l'espressione regolare nei percorsi, attiva questa opzione se desideri eseguire la corrispondenza delle espressioni regolari AWS WAF per le specifiche del percorso della pagina di accesso.

      AWS WAF supporta la sintassi del pattern utilizzata dalla libreria `libpcre` PCRE con alcune eccezioni. La libreria è documentata in PCRE - Perl Compatible Regular Expressions. Per informazioni sul AWS WAF supporto, vedere. Corrispondenza dei modelli di espressioni regolari in AWS WAF

   b. Per Percorso di accesso, fornisci il percorso dell'endpoint di accesso per l'applicazione. Il gruppo di regole esamina solo le `POST` richieste HTTP all'endpoint di accesso specificato.

      > **Note**
      >
      > La corrispondenza per gli endpoint non fa distinzione tra maiuscole e minuscole. Le specifiche Regex non devono contenere il flag`(?-i)`, che disabilita la corrispondenza senza distinzione tra maiuscole e minuscole. Le specifiche delle stringhe devono iniziare con una barra. `/`

      Ad esempio, per l'URL`https://example.com/web/login`, è possibile fornire la specifica `/web/login` del percorso della stringa. I percorsi di accesso che iniziano con il percorso fornito sono considerati corrispondenti. Ad esempio `/web/login` corrisponde ai percorsi di accesso `/web/login/web/login/`,`/web/loginPage`, e`/web/login/thisPage`, ma non corrisponde al percorso di accesso `/home/web/login` o`/website/login`.

   c. Per Request inspection, specifica in che modo l'applicazione accetta i tentativi di accesso fornendo il tipo di payload della richiesta e i nomi dei campi all'interno del corpo della richiesta in cui vengono forniti il nome utente e la password. La specificazione dei nomi dei campi dipende dal tipo di payload.

- Tipo di payload JSON: specifica i nomi dei campi nella sintassi del puntatore JSON. Per informazioni sulla sintassi JSON Pointer, consultate la documentazione di Internet Engineering Task Force (IETF) Object Notation (JSON) Pointer. JavaScript

  Ad esempio, per l'esempio seguente JSON payload, la specifica del campo nome utente è e la specifica del campo password è. `/login/username` `/login/password`

  ```
  {
      "login": {
          "username": "THE_USERNAME",
          "password": "THE_PASSWORD"
      }
  }
  ```

- Tipo di payload FORM_ENCODED: utilizza i nomi dei moduli HTML.

  Ad esempio, per un modulo HTML con elementi di input denominati `username1` e`password1`, la specifica del campo nome utente è `username1` e la specifica del campo password è. `password1`

d. Se stai proteggendo CloudFront le distribuzioni Amazon, nella sezione Controllo Response, specifica in che modo l'applicazione indica l'esito positivo o negativo delle risposte ai tentativi di accesso.

> **Note**
>
> L'ispezione della risposta ATP è disponibile solo negli ACL Web che proteggono le distribuzioni. CloudFront

Specificate un singolo componente nella risposta di accesso che desiderate che l'ATP controlli. Per i tipi di componenti Body e JSON, AWS WAF può ispezionare i primi 65.536 byte (64 KB) del componente.

Fornite i criteri di ispezione per il tipo di componente, come indicato dall'interfaccia. È necessario fornire i criteri di successo e di fallimento da ispezionare nel componente.

Ad esempio, supponiamo che l'applicazione indichi lo stato di un tentativo di accesso nel codice di stato della risposta e lo utilizzi `200 OK` come esito positivo `401 Unauthorized` e/o `403 Forbidden` negativo. Dovreste impostare il tipo di componente di ispezione della

risposta su Codice di stato, quindi nella casella di testo Operazione riuscita immettete `200` e nella casella di testo Errore immettete `401` sulla prima riga e `403` sulla seconda.

Il gruppo di regole ATP conta solo le risposte che soddisfano i criteri di ispezione con esito positivo o negativo. Le regole del gruppo di regole agiscono sui clienti quando hanno un tasso di fallimento troppo elevato tra le risposte conteggiate. Per un comportamento accurato in base alle regole del gruppo di regole, assicurati di fornire informazioni complete sia per i tentativi di accesso riusciti che per quelli non riusciti.

Per vedere le regole che controllano le risposte di accesso, cerca `VolumetricIpFailedLoginResponseHigh` e `VolumetricSessionFailedLoginResponseHigh` nell'elenco delle regole in[AWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi](#).

3. Fornisci qualsiasi configurazione aggiuntiva che desideri per il gruppo di regole.

   È possibile limitare ulteriormente l'ambito delle richieste esaminate dal gruppo di regole aggiungendo un'istruzione scope-down all'istruzione del gruppo di regole gestito. Ad esempio, è possibile esaminare solo le richieste con un argomento di interrogazione o un cookie specifico. Il gruppo di regole esaminerà solo `POST` le richieste HTTP all'endpoint di accesso specificato che corrispondono ai criteri dell'istruzione scope-down. Per informazioni sulle istruzioni scope-down, vedere. [Dichiarazioni delimitate](#)

4. Salvate le modifiche nell'ACL Web.

Prima di implementare l'implementazione ATP per il traffico di produzione, testala e ottimizzala in un ambiente di staging o test finché non ti senti a tuo agio con il potenziale impatto sul traffico. Quindi testate e ottimizzate le regole in modalità di conteggio in base al traffico di produzione prima di attivarle. Per informazioni, consulta la sezione che segue.

Test e implementazione dell'ATP

Questa sezione fornisce linee guida generali per configurare e testare un'implementazione di AWS WAF Fraud Control Account Takeover Prevention (ATP) per il tuo sito. I passaggi specifici che sceglierete di seguire dipenderanno dalle vostre esigenze, dalle risorse e dalle richieste web che riceverete.

Queste informazioni si aggiungono alle informazioni generali su test e ottimizzazione fornite all'indirizzo[Test e ottimizzazione delle protezioni AWS WAF](#).

> **Note**
>
> AWS Le Managed Rules sono progettate per proteggerti dalle minacce web più comuni. Se utilizzati in conformità con la documentazione, i gruppi di regole AWS Managed Rules aggiungono un altro livello di sicurezza per le applicazioni. Tuttavia, i gruppi di regole AWS Managed Rules non sono intesi come sostituti delle responsabilità in materia di sicurezza, che sono determinate dalle AWS risorse selezionate. Fai riferimento al modello di responsabilità condivisa per assicurarti che le tue risorse AWS siano adeguatamente protette.

> **Rischio legato al traffico di produzione**
>
> Prima di implementare l'implementazione ATP per il traffico di produzione, testala e ottimizzala in un ambiente di staging o di test finché non ti senti a tuo agio con il potenziale impatto sul traffico. Quindi testate e ottimizzate le regole in modalità di conteggio in base al traffico di produzione prima di attivarle.

AWS WAF fornisce credenziali di test che è possibile utilizzare per verificare la configurazione ATP. Nella procedura seguente, configurerai un ACL web di prova per utilizzare il gruppo di regole gestito ATP, configurerai una regola per acquisire l'etichetta aggiunta dal gruppo di regole e quindi eseguirai un tentativo di accesso utilizzando queste credenziali di test. Verificherai che il tuo ACL web abbia gestito correttamente il tentativo controllando i CloudWatch parametri di Amazon per il tentativo di accesso.

Questa guida è destinata agli utenti che sanno in generale come creare e gestire ACL AWS WAF Web, regole e gruppi di regole. Questi argomenti sono trattati nelle sezioni precedenti di questa guida.

Per configurare e testare un'implementazione di AWS WAF Fraud Control Account Takeover Prevention (ATP)

Esegui questi passaggi prima in un ambiente di test, poi in produzione.

1. Aggiungi il gruppo di regole gestito per la prevenzione dell'acquisizione di account (ATP) di AWS WAF Fraud Control in modalità count

   > **Note**
   >
   > Quando utilizzi questo gruppo di regole gestito, ti vengono addebitati costi aggiuntivi. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

   Aggiungi il gruppo di regole AWS Managed Rules `AWSManagedRulesATPRuleSet` a un ACL web nuovo o esistente e configuralo in modo che non alteri il comportamento corrente dell'ACL web. Per informazioni dettagliate sulle regole e le etichette per questo gruppo di regole, consulta. AWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi

   - Quando aggiungi il gruppo di regole gestito, modificalo e procedi come segue:
     - Nel riquadro di configurazione del gruppo di regole, fornisci i dettagli della pagina di accesso dell'applicazione. Il gruppo di regole ATP utilizza queste informazioni per monitorare le attività di accesso. Per ulteriori informazioni, consulta Aggiungere il gruppo di regole gestite da ATP all'ACL Web.
     - Nel riquadro Regole, apri il menu a discesa Sostituisci tutte le azioni delle regole e scegli. Count Con questa configurazione, AWS WAF valuta le richieste in base a tutte le regole del gruppo di regole e conta solo le corrispondenze risultanti, pur continuando ad aggiungere etichette alle richieste. Per ulteriori informazioni, consulta Sovrascrivere le azioni delle regole in un gruppo di regole.

       Con questo override, è possibile monitorare il potenziale impatto delle regole gestite da ATP per determinare se aggiungere eccezioni, ad esempio eccezioni per casi d'uso interni.
   - Posiziona il gruppo di regole in modo che venga valutato in base alle regole esistenti nell'ACL Web, con un'impostazione di priorità numericamente superiore a qualsiasi regola o gruppo di regole che stai già utilizzando. Per ulteriori informazioni, consulta Ordine di elaborazione delle regole e dei gruppi di regole in un ACL Web.

     In questo modo, la tua attuale gestione del traffico non viene interrotta. Ad esempio, se hai regole che rilevano il traffico dannoso come SQL injection o cross-site scripting, continueranno a rilevarlo e registrarlo. In alternativa, se esistono regole che consentono il traffico noto e non dannoso, queste possono continuare a consentire tale traffico senza che venga bloccato

dal gruppo di regole gestito dall'ATP. Potresti decidere di modificare l'ordine di elaborazione durante le attività di test e ottimizzazione.

2. Abilita il campionamento, la registrazione e le metriche per l'ACL web

   Se necessario, configura la registrazione per l'ACL Web e abilita il campionamento e i parametri Amazon. CloudWatch Puoi utilizzare questi strumenti di visibilità per monitorare l'interazione del gruppo di regole gestito da ATP con il tuo traffico.

   - Per informazioni sulla configurazione e l'utilizzo della registrazione, vedere. Registrazione del traffico AWS WAF ACL Web
   - Per informazioni sui CloudWatch parametri di Amazon, consultaMonitoraggio con Amazon CloudWatch.
   - Per informazioni sul campionamento delle richieste web, consulta. Visualizzazione di un esempio di richieste Web

3. Associare l'ACL Web a una risorsa

   Se l'ACL web non è già associato a una risorsa di test, associala. Per informazioni, consulta Associazione o dissociazione di un ACL Web con una risorsa AWS.

4. Monitora il traffico e la corrispondenza delle regole ATP

   Assicurati che il traffico sia regolare e che le regole del gruppo di regole gestite da ATP aggiungano etichette alle richieste web corrispondenti. Puoi vedere le etichette nei log e vedere i parametri ATP e delle etichette nei parametri di Amazon. CloudWatch Nei log, le regole che hai sostituito per conteggiare nel gruppo di regole vengono visualizzate nel comando `ruleGroupList` con `action` set to count e `overriddenAction` indicano l'azione della regola configurata che hai ignorato.

5. Verifica le funzionalità di controllo delle credenziali del gruppo di regole

   Esegui un tentativo di accesso con le credenziali di test compromised e verifica che il gruppo di regole corrisponda a tali credenziali come previsto.

   a. Accedi alla pagina di accesso della risorsa protetta utilizzando la seguente coppia di credenziali AWS WAF di test:

      - Utente: `WAF_TEST_CREDENTIAL@wafexample.com`
      - Password: `WAF_TEST_CREDENTIAL_PASSWORD`

Queste credenziali di test sono classificate come credenziali compromesse e il gruppo di regole gestite ATP aggiungerà l'`awswaf:managed:aws:atp:signal:credential_compromised`etichetta alla richiesta di accesso, che puoi vedere nei log.

b. Nei registri ACL Web, cerca l'`awswaf:managed:aws:atp:signal:credential_compromised`etichetta nel `labels` campo delle voci di registro per le richieste web di accesso di prova. Per ulteriori informazioni sulla registrazione, consulta Registrazione del traffico AWS WAF ACL Web.

Dopo aver verificato che il gruppo di regole acquisisca le credenziali compromesse come previsto, puoi adottare le misure necessarie per configurarne l'implementazione in base alle tue esigenze per la risorsa protetta.

6. Per le CloudFront distribuzioni, prova la gestione degli errori di accesso del gruppo di regole

a. Esegui un test per ogni criterio di risposta agli errori configurato per il gruppo di regole ATP. Attendi almeno 10 minuti tra un test e l'altro.

Per testare un singolo criterio di errore, identifica un tentativo di accesso che abbia esito negativo con quel criterio nella risposta. Quindi, da un singolo indirizzo IP del client, esegui almeno 10 tentativi di accesso falliti in meno di 10 minuti.

Dopo i primi 6 errori, la regola volumetrica di accesso fallito dovrebbe iniziare a corrispondere agli altri tentativi, etichettandoli e contandoli. La regola potrebbe non rispettare i primi uno o due a causa della latenza.

b. Nei registri ACL Web, cerca l'`awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high` nel `labels` campo delle voci di registro per le richieste web di accesso di prova. Per ulteriori informazioni sulla registrazione, consulta Registrazione del traffico AWS WAF ACL Web.

Questi test verificano che i criteri di errore corrispondano alle risposte fornite, verificando che il numero di accessi non riusciti superi le soglie stabilite dalla regola. `VolumetricIpFailedLoginResponseHigh` Una volta raggiunte le soglie, se continui a inviare richieste di accesso dallo stesso indirizzo IP, la regola continuerà a corrispondere fino a

quando la percentuale di errori non scenderà al di sotto della soglia. Sebbene le soglie vengano superate, la regola corrisponde sia agli accessi riusciti che a quelli non riusciti dall'indirizzo IP.

7. Personalizza la gestione delle richieste web ATP

   Se necessario, aggiungi le tue regole che consentono o bloccano esplicitamente le richieste, per modificare il modo in cui le regole ATP le gestirebbero altrimenti.

   Ad esempio, puoi utilizzare le etichette ATP per consentire o bloccare le richieste o per personalizzare la gestione delle richieste. È possibile aggiungere una regola di corrispondenza delle etichette dopo il gruppo di regole gestite ATP per filtrare le richieste etichettate in base alla gestione che si desidera applicare. Dopo il test, mantieni le regole ATP correlate in modalità di conteggio e mantieni le decisioni sulla gestione delle richieste nella tua regola personalizzata. Per vedere un esempio, consulta Esempio ATP: gestione personalizzata delle credenziali mancanti e compromesse.

8. Rimuovi le regole del test e abilita le impostazioni del gruppo di regole gestite ATP

   A seconda della situazione, potresti aver deciso di lasciare alcune regole ATP in modalità count. Per le regole che desideri eseguire secondo la configurazione configurata all'interno del gruppo di regole, disabilita la modalità di conteggio nella configurazione del gruppo di regole ACL Web. Al termine del test, puoi anche rimuovere le regole di corrispondenza delle etichette di test.

9. Monitora e sintonizza

   Per assicurarti che le richieste web vengano gestite come desideri, monitora attentamente il traffico dopo aver abilitato la funzionalità ATP che intendi utilizzare. Modificate il comportamento in base alle esigenze applicando le regole (rules count override) sul gruppo di regole e con le vostre regole.

Dopo aver terminato il test dell'implementazione del gruppo di regole ATP, se non l'hai già fatto, ti consigliamo vivamente di integrare l' AWS WAF JavaScript SDK nella pagina di accesso del browser, per funzionalità di rilevamento avanzate. AWS WAF fornisce anche SDK mobili per integrare dispositivi iOS e Android. Per ulteriori informazioni sugli SDK di integrazione, consulta. AWS WAF integrazione delle applicazioni client Per informazioni su questa raccomandazione, consultaPerché dovresti usare gli SDK di integrazione delle applicazioni con ATP.

AWS WAF Esempi di prevenzione dell'acquisizione di account (ATP) per il controllo delle frodi

Questa sezione mostra configurazioni di esempio che soddisfano i casi d'uso più comuni per le implementazioni di AWS WAF Fraud Control Account Takeover Prevention (ATP).

Ogni esempio fornisce una descrizione del caso d'uso e quindi mostra la soluzione negli elenchi JSON per le regole configurate personalizzate.

> **Note**
>
> È possibile recuperare elenchi JSON come quelli mostrati in questi esempi tramite il download web ACL JSON della console o l'editor JSON delle regole, oppure tramite l'`getWebACL`operazione nelle API e nell'interfaccia a riga di comando.

Argomenti

- Esempio ATP: configurazione semplice
- Esempio ATP: gestione personalizzata delle credenziali mancanti e compromesse
- Esempio ATP: configurazione dell'ispezione della risposta

Esempio ATP: configurazione semplice

Il seguente elenco JSON mostra un esempio di ACL web con un gruppo di regole gestito per la prevenzione dell'acquisizione di account (ATP) di AWS WAF Fraud Control. Nota la configurazione aggiuntiva della pagina di accesso, che fornisce al gruppo di regole le informazioni necessarie per monitorare e gestire le richieste di accesso. Questo codice JSON include le impostazioni generate automaticamente dall'ACL Web, come lo spazio dei nomi delle etichette e l'URL di integrazione dell'applicazione dell'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"
}
```

Esempio ATP: gestione personalizzata delle credenziali mancanti e compromesse

Per impostazione predefinita, i controlli delle credenziali eseguiti dal gruppo di regole `AWSManagedRulesATPRuleSet` gestiscono le richieste Web nel modo seguente:

- Credenziali mancanti: etichetta e blocca la richiesta.
- Credenziali compromesse: etichetta la richiesta ma non bloccarla o contarla.

Per informazioni dettagliate sul gruppo di regole e sul comportamento delle regole, consulta. AWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi

È possibile aggiungere una gestione personalizzata per le richieste Web con credenziali mancanti o compromesse effettuando le seguenti operazioni:

- Sostituisci la **`MissingCredential`** regola conCount: questa modifica dell'azione della regola fa sì che la regola conteggi ed etichetta solo le richieste corrispondenti.
- Aggiungi una regola di corrispondenza delle etichette con gestione personalizzata: configura questa regola in modo che corrisponda a entrambe le etichette ATP e per eseguire la gestione personalizzata. Ad esempio, potresti reindirizzare il cliente alla tua pagina di registrazione.

La regola seguente mostra il gruppo di regole gestite ATP dell'esempio precedente, con l'azione della `MissingCredential` regola sostituita dal conteggio. Ciò fa sì che la regola applichi la propria etichetta alle richieste corrispondenti e quindi conti solo le richieste, invece di bloccarle.

```
"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 questa configurazione, quando questo gruppo di regole valuta una richiesta Web con credenziali mancanti o compromesse, etichetterà la richiesta, ma non la bloccherà.

La regola seguente ha un'impostazione di priorità numericamente superiore rispetto al gruppo di regole precedente. AWS WAF valuta le regole in ordine numerico, a partire dalla più bassa, quindi questa regola verrà valutata dopo la valutazione del gruppo di regole. La regola è configurata per corrispondere a entrambe le etichette delle credenziali e per inviare una risposta personalizzata per le richieste corrispondenti.

```
"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"
      }
```

Esempio ATP: configurazione dell'ispezione della risposta

Il seguente elenco JSON mostra un esempio di ACL web con un gruppo di regole gestito per la prevenzione dell'acquisizione di account (ATP) di AWS WAF Fraud Control configurato per controllare le risposte di origine. Nota la configurazione dell'ispezione delle risposte, che specifica i codici di esito positivo e dello stato della risposta. Puoi anche configurare le impostazioni di successo e risposta in base alle corrispondenze JSON di header, body e body. Questo codice JSON include le impostazioni generate automaticamente dall'ACL Web, come lo spazio dei nomi delle etichette e l'URL di integrazione dell'applicazione dell'ACL Web.

> **Note**
>
> L'ispezione della risposta ATP è disponibile solo negli ACL Web che proteggono le distribuzioni. CloudFront

```
{
    "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 Controllo dei bot

Con Bot Control, puoi facilmente monitorare, bloccare o limitare la velocità di bot come scraper, scanner, crawler, monitor di stato e motori di ricerca. Se utilizzi il livello di ispezione mirato del gruppo di regole, puoi anche sfidare i bot che non si identificano automaticamente, rendendo più difficile e costoso per i bot malintenzionati operare contro il tuo sito web. Puoi proteggere le tue applicazioni utilizzando il gruppo di regole gestito di Bot Control da solo o in combinazione con altri gruppi di regole AWS Managed Rules e regole personalizzate AWS WAF .

Bot Control include una console di controllo che mostra la quantità di traffico attuale proveniente dai bot, in base al campionamento delle richieste. Con il gruppo di regole gestito da Bot Control aggiunto al tuo ACL web, puoi intervenire contro il traffico dei bot e ricevere informazioni dettagliate e in tempo reale sul traffico di bot comune che arriva alle tue applicazioni.

> **Note**
>
> Quando utilizzi questo gruppo di regole gestito, ti vengono addebitati costi aggiuntivi. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

Il gruppo di regole gestito da Bot Control fornisce un livello di protezione di base comune che aggiunge etichette ai bot che si identificano automaticamente, verifica i bot generalmente desiderati e rileva le firme dei bot ad alta affidabilità. Questo ti dà la possibilità di monitorare e controllare le categorie comuni di traffico dei bot.

Il gruppo di regole Bot Control fornisce anche un livello di protezione mirato che aggiunge il rilevamento di bot sofisticati che non si identificano automaticamente. Le protezioni mirate utilizzano tecniche di rilevamento come l'interrogazione del browser, il rilevamento delle impronte digitali e l'euristica comportamentale per identificare il traffico di bot non valido. Inoltre, le protezioni mirate forniscono un'analisi opzionale automatizzata e basata sull'apprendimento automatico delle statistiche sul traffico del sito Web per rilevare le attività relative ai bot. Quando abiliti l'apprendimento automatico, AWS WAF utilizza le statistiche sul traffico del sito Web, come timestamp, caratteristiche del browser e URL visitato in precedenza, per migliorare il modello di apprendimento automatico di Bot Control.

Per ulteriori informazioni sul gruppo di regole gestito da Bot Control, consulta. AWS WAF Gruppo di regole Bot Control

Quando AWS WAF valuta una richiesta web rispetto al gruppo di regole gestito da Bot Control, il gruppo di regole aggiunge etichette alle richieste che rileva come correlate al bot, ad esempio la categoria del bot e il nome del bot. Puoi abbinarle a queste etichette nelle tue AWS WAF regole per personalizzare la gestione. Le etichette generate dal gruppo di regole gestito da Bot Control sono incluse nelle CloudWatch metriche di Amazon e nei log ACL Web.

Puoi anche utilizzare AWS Firewall Manager AWS WAF le policy per distribuire il gruppo di regole gestito da Bot Control tra le tue applicazioni in più account che fanno parte della tua organizzazione. AWS Organizations

Componenti Bot Control

I componenti principali di un'implementazione di Bot Control sono i seguenti:

- **`AWSManagedRulesBotControlRuleSet`**— Il gruppo di regole gestito da Bot Control le cui regole rilevano e gestiscono varie categorie di bot. Questo gruppo di regole aggiunge etichette alle richieste web che rileva come traffico di bot.

  > **Note**
  >
  > Quando utilizzi questo gruppo di regole gestito, ti vengono addebitati costi aggiuntivi. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

  Il gruppo di regole gestito da Bot Control offre due livelli di protezione tra cui puoi scegliere:

  - Comune: rileva una varietà di bot che si identificano automaticamente, come framework di web scraping, motori di ricerca e browser automatici. Le protezioni Bot Control a questo livello identificano i bot più comuni utilizzando tecniche di rilevamento dei bot tradizionali, come l'analisi statica dei dati delle richieste. Le regole etichettano il traffico proveniente da questi bot e bloccano quello che non possono verificare.
  - Mirato: include le protezioni di livello comune e aggiunge il rilevamento mirato per bot sofisticati che non si identificano automaticamente. Le protezioni mirate mitigano l'attività dei bot utilizzando una combinazione di limitazioni della velocità e sfide legate al CAPTCHA e al browser in background.

- **`TGT_`**— Le regole che forniscono una protezione mirata hanno nomi che iniziano con. `TGT_` Tutte le protezioni mirate utilizzano tecniche di rilevamento come l'interrogazione del browser, l'impronta digitale e l'euristica comportamentale per identificare il traffico di bot non valido.
- **`TGT_ML_`**— Le regole di protezione mirate che utilizzano l'apprendimento automatico hanno nomi che iniziano con. `TGT_ML_` Queste regole utilizzano l'analisi automatizzata e basata sull'apprendimento automatico delle statistiche sul traffico dei siti Web per rilevare comportamenti anomali indicativi di un'attività distribuita e coordinata dei bot. AWS WAF analizza le statistiche sul traffico del sito Web, ad esempio timestamp, caratteristiche del browser e URL visitato in precedenza, per migliorare il modello di apprendimento automatico di Bot Control. Le funzionalità di machine learning sono abilitate per impostazione predefinita, ma puoi disabilitarle nella configurazione del gruppo di regole. Quando l'apprendimento automatico è disabilitato, AWS WAF non valuta queste regole.

Per ulteriori dettagli, incluse informazioni sulle regole del gruppo di regole, vedereAWS WAF Gruppo di regole Bot Control.

È possibile includere questo gruppo di regole nell'ACL Web utilizzando una dichiarazione di riferimento per il gruppo di regole gestite e indicando il livello di ispezione che si desidera utilizzare. Per il livello di destinazione, indichi anche se abilitare l'apprendimento automatico. Per ulteriori informazioni sull'aggiunta di questo gruppo di regole gestito all'ACL Web, consultaAggiungere il gruppo di regole gestito da AWS WAF Bot Control all'ACL web.

- Bot Control Dashboard: la dashboard di monitoraggio dei bot per il tuo ACL web, disponibile tramite la scheda web ACL Bot Control. Usa questa dashboard per monitorare il traffico e capire in che misura proviene da vari tipi di bot. Questo può essere un punto di partenza per personalizzare la gestione dei bot, come descritto in questo argomento. Puoi anche usarlo per verificare le modifiche e monitorare l'attività di vari bot e categorie di bot.
- JavaScript e SDK per l'integrazione di applicazioni mobili: dovresti implementare gli AWS WAF JavaScript SDK per dispositivi mobili se utilizzi il livello di protezione mirato del gruppo di regole Bot Control. Le regole mirate utilizzano le informazioni fornite dagli SDK nei token client per un rilevamento avanzato contro i bot dannosi. Per ulteriori informazioni sugli SDK, consulta AWS WAF integrazione delle applicazioni client.
- Registrazione e metriche: puoi monitorare il traffico dei bot e capire come il gruppo di regole gestito da Bot Control valuta e gestisce il tuo traffico studiando i log e le metriche CloudWatch Amazon per il tuo ACL web. Le etichette che Bot Control aggiunge alle tue richieste web sono incluse nei log e nelle CloudWatch metriche di Amazon. Per informazioni sulla configurazione e l'utilizzo di log

e metriche, consulta e. Registrazione del traffico AWS WAF ACL Web Monitoraggio con Amazon CloudWatch

A seconda delle tue esigenze e del traffico registrato, potresti voler personalizzare l'implementazione di Bot Control. Di seguito sono riportate alcune delle opzioni più utilizzate.

- Istruzioni Scope-down: puoi escludere parte del traffico dalle richieste Web valutate dal gruppo di regole gestito da Bot Control aggiungendo un'istruzione scope-down all'interno dell'istruzione di riferimento del gruppo di regole gestito da Bot Control. Un'istruzione scope-down può essere qualsiasi istruzione di regola nestable. Quando una richiesta non corrisponde all'istruzione scope-down, la AWS WAF valuta come non corrispondente all'istruzione di riferimento del gruppo di regole senza valutarla rispetto al gruppo di regole. Per ulteriori informazioni sulle istruzioni scope-down, vedere. Dichiarazioni delimitate

  I prezzi per il gruppo di regole gestito da Bot Control aumentano in base al numero di richieste Web che AWS WAF vengono valutate in base al gruppo. Puoi contribuire a ridurre questi costi utilizzando un'istruzione scope-down per limitare le richieste valutate dal gruppo di regole. Ad esempio, potresti voler consentire il caricamento della tua home page per tutti, bot inclusi, e quindi applicare le regole del gruppo di regole alle richieste che vanno alle API dell'applicazione o che contengono un particolare tipo di contenuto.
- Etichette e regole di corrispondenza delle etichette: puoi personalizzare il modo in cui il gruppo di regole Bot Control gestisce parte del traffico bot che identifica utilizzando l'istruzione AWS WAF label match rule. Il gruppo di regole Bot Control aggiunge etichette alle tue richieste web. Puoi aggiungere regole di corrispondenza delle etichette dopo il gruppo di regole Bot Control che corrispondono alle etichette di Bot Control e applicare la gestione di cui hai bisogno. Per ulteriori informazioni sull'etichettatura e sull'utilizzo delle istruzioni di abbinamento delle etichette, consulta Dichiarazione della regola di corrispondenza delle etichette eAWS WAF etichette sulle richieste web.
- Richieste e risposte personalizzate: puoi aggiungere intestazioni personalizzate alle richieste consentite e inviare risposte personalizzate per le richieste che blocchi abbinando l'etichetta alle funzionalità di richiesta e risposta AWS WAF personalizzate. Per ulteriori informazioni sulla personalizzazione di richieste e risposte, consulta. Richieste e risposte web personalizzate in AWS WAF

Perché dovresti usare gli SDK di integrazione delle applicazioni con Bot Control

La maggior parte delle protezioni mirate del gruppo di regole gestito da Bot Control richiede i token di sfida generati dagli SDK di integrazione delle applicazioni. Le regole che non richiedono un token di

sfida sulla richiesta sono le protezioni di livello comune di Bot Control e le regole di machine learning di livello mirato. Per le descrizioni dei livelli di protezione e delle regole nel gruppo di regole, vediAWS WAF Gruppo di regole Bot Control.

Consigliamo vivamente di implementare gli SDK di integrazione delle applicazioni, per un uso più efficace del gruppo di regole Bot Control. Lo script di sfida deve essere eseguito prima del gruppo di regole Bot Control affinché il gruppo di regole possa beneficiare dei token acquisiti dallo script.

- Con gli SDK di integrazione delle applicazioni, lo script viene eseguito automaticamente.
- Se non riesci a utilizzare gli SDK, puoi configurare l'ACL web in modo che esegua l'azione Challenge o CAPTCHA regola tutte le richieste che verranno esaminate dal gruppo di regole Bot Control. L'utilizzo dell'azione Challenge o CAPTCHA rule può comportare costi aggiuntivi. Per i dettagli sui prezzi, vedere Prezzi di AWS WAF.

Quando implementate gli SDK di integrazione delle applicazioni nei vostri client o utilizzate una delle azioni delle regole che eseguono lo script di sfida, espandete le funzionalità del gruppo di regole e della sicurezza complessiva delle applicazioni client.

I token forniscono informazioni sui clienti con ogni richiesta web. Queste informazioni aggiuntive consentono al gruppo di regole Bot Control di separare le sessioni client legittime dalle sessioni client che si comportano male, anche se entrambe provengono da un unico indirizzo IP. Il gruppo di regole utilizza le informazioni contenute nei token per aggregare il comportamento delle richieste di sessione del client per il rilevamento e la mitigazione ottimizzati forniti dal livello di protezione mirato.

Per informazioni sugli SDK, consulta. AWS WAF integrazione delle applicazioni client Per informazioni sui AWS WAF token, consulta. AWS WAF token di richiesta web Per informazioni sulle azioni delle regole, vedereCAPTCHAe Challenge in AWS WAF.

Aggiungere il gruppo di regole gestito da AWS WAF Bot Control all'ACL web

Il gruppo di regole gestito da Bot Control `AWSManagedRulesBotControlRuleSet` richiede una configurazione aggiuntiva per identificare il livello di protezione che si desidera implementare.

Per la descrizione del gruppo di regole e l'elenco delle regole, vediAWS WAF Gruppo di regole Bot Control.

Questa guida è destinata agli utenti che sanno in generale come creare e gestire ACL AWS WAF Web, regole e gruppi di regole. Questi argomenti sono trattati nelle sezioni precedenti di questa

guida. Per informazioni di base su come aggiungere un gruppo di regole gestito all'ACL Web, consultaAggiungere un gruppo di regole gestito a un ACL Web tramite la console.

Segui le migliori pratiche

Utilizza il gruppo di regole Bot Control in conformità con le best practice riportate inLe migliori pratiche per la mitigazione intelligente delle minacce.

Per utilizzare il gruppo di **`AWSManagedRulesBotControlRuleSet`** regole nella tua ACL web

1. Aggiungi il gruppo di regole AWS gestito `AWSManagedRulesBotControlRuleSet` all'ACL web. Per la descrizione completa del gruppo di regole, consultathe section called “Gruppo di regole Bot Control”.

   > **Note**
   >
   > Quando utilizzi questo gruppo di regole gestito, ti vengono addebitati costi aggiuntivi. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

   Quando aggiungi il gruppo di regole, modificalo per aprire la pagina di configurazione per il gruppo di regole.
2. Nella pagina di configurazione del gruppo di regole, nel riquadro Livello di ispezione, seleziona il livello di ispezione che desideri utilizzare.

   - Comune: rileva una varietà di bot che si identificano automaticamente, come framework di web scraping, motori di ricerca e browser automatici. Le protezioni Bot Control a questo livello identificano i bot più comuni utilizzando tecniche di rilevamento dei bot tradizionali, come l'analisi statica dei dati delle richieste. Le regole etichettano il traffico proveniente da questi bot e bloccano quello che non possono verificare.
   - Mirato: include le protezioni di livello comune e aggiunge il rilevamento mirato per bot sofisticati che non si identificano automaticamente. Le protezioni mirate mitigano l'attività dei bot utilizzando una combinazione di limitazioni della velocità e sfide legate al CAPTCHA e al browser in background.
     - **`TGT_`**— Le regole che forniscono una protezione mirata hanno nomi che iniziano con. `TGT_` Tutte le protezioni mirate utilizzano tecniche di rilevamento come l'interrogazione del browser, il rilevamento delle impronte digitali e l'euristica comportamentale per identificare il traffico di bot non valido.

- **`TGT_ML_`**— Le regole di protezione mirate che utilizzano l'apprendimento automatico hanno nomi che iniziano con. `TGT_ML_` Queste regole utilizzano l'analisi automatizzata e basata sull'apprendimento automatico delle statistiche sul traffico dei siti Web per rilevare comportamenti anomali indicativi di un'attività distribuita e coordinata dei bot. AWS WAF analizza le statistiche sul traffico del sito Web, ad esempio timestamp, caratteristiche del browser e URL visitato in precedenza, per migliorare il modello di apprendimento automatico di Bot Control. Le funzionalità di machine learning sono abilitate per impostazione predefinita, ma puoi disabilitarle nella configurazione del gruppo di regole. Quando l'apprendimento automatico è disabilitato, AWS WAF non valuta queste regole.

3. Se utilizzi il livello di protezione mirato e non desideri AWS WAF utilizzare l'apprendimento automatico (ML) per analizzare il traffico web alla ricerca di attività di bot distribuite e coordinate, disattiva l'opzione di apprendimento automatico. L'apprendimento automatico è necessario per le regole di Bot Control i cui nomi iniziano con`TGT_ML_`. Per informazioni dettagliate su queste regole, consultaElenco delle regole di Bot Control.
4. Aggiungere un'istruzione riassuntiva per il gruppo di regole, per contenere i costi del suo utilizzo. Un'istruzione riportata verso il basso restringe l'insieme di richieste esaminate dal gruppo di regole. Ad esempio, casi d'uso, inizia con e. Esempio di Bot Control: usa Bot Control solo per la pagina di accesso Esempio di Bot Control: utilizza Bot Control solo per contenuti dinamici
5. Fornisci qualsiasi configurazione aggiuntiva necessaria per il gruppo di regole.
6. Salva le modifiche nell'ACL web.

Prima di implementare l'implementazione di Bot Control per il traffico di produzione, testala e ottimizzala in un ambiente di staging o di test finché non ti senti a tuo agio con il potenziale impatto sul traffico. Quindi testa e ottimizza le regole in modalità di conteggio in base al traffico di produzione prima di attivarle. Per ulteriori informazioni, consulta le sezioni seguenti.

Falsi positivi con AWS WAF Bot Control

Abbiamo selezionato con cura le regole del gruppo di regole gestito da AWS WAF Bot Control per ridurre al minimo i falsi positivi. Testiamo le regole rispetto al traffico globale e ne monitoriamo l'impatto sugli ACL web di prova. Tuttavia, è ancora possibile ottenere falsi positivi a causa di cambiamenti nei modelli di traffico. Inoltre, è noto che alcuni casi d'uso causano falsi positivi e richiedono una personalizzazione specifica per il traffico web.

Le situazioni in cui è possibile riscontrare falsi positivi includono:

- Le app per dispositivi mobili in genere hanno agenti utente diversi dal browser, che la `SignalNonBrowserUserAgent` regola blocca per impostazione predefinita. Se ti aspetti traffico proveniente da app per dispositivi mobili o qualsiasi altro traffico legittimo con agenti utente diversi dal browser, dovrai aggiungere un'eccezione per consentirlo.
- Potresti fare affidamento su un traffico bot specifico per cose come il monitoraggio dell'uptime, i test di integrazione o gli strumenti di marketing. Se Bot Control identifica e blocca il traffico bot che desideri consentire, devi modificare la gestione aggiungendo regole personalizzate. Sebbene non si tratti di uno scenario di falso positivo per tutti i clienti, se lo è per te, dovrai gestirlo come per un falso positivo.
- Il gruppo di regole gestito da Bot Control verifica i bot utilizzando gli indirizzi IP di. AWS WAF Se utilizzi Bot Control e hai verificato i bot che effettuano il routing attraverso un proxy o un sistema di bilanciamento del carico, potresti dover autorizzarli esplicitamente utilizzando una regola personalizzata. Per informazioni su come creare una regola personalizzata di questo tipo, consulta. Indirizzo IP inoltrato
- Una regola di Bot Control con una bassa percentuale globale di falsi positivi potrebbe avere un forte impatto su dispositivi o applicazioni specifici. Ad esempio, durante i test e la convalida, potremmo non aver osservato le richieste provenienti da applicazioni con bassi volumi di traffico o da browser o dispositivi meno comuni.
- Una regola di Bot Control con un tasso di falsi positivi storicamente basso potrebbe aver aumentato i falsi positivi per il traffico valido. Ciò potrebbe essere dovuto a nuovi modelli di traffico o agli attributi di richiesta che emergono con il traffico valido, che fanno sì che il traffico corrisponda alla regola laddove prima non corrispondeva. Queste modifiche potrebbero essere dovute a situazioni come le seguenti:
  - Dettagli sul traffico che vengono alterati man mano che il traffico scorre attraverso le appliance di rete, come i sistemi di bilanciamento del carico o le reti di distribuzione dei contenuti (CDN).
  - Modifiche emergenti nei dati sul traffico, ad esempio nuovi browser o nuove versioni per i browser esistenti.

Per informazioni su come gestire i falsi positivi che potresti ottenere dal gruppo di regole gestito da AWS WAF Bot Control, consulta le indicazioni nella sezione che segue,Test e implementazione di AWS WAF Bot Control.

Test e implementazione di AWS WAF Bot Control

Questa sezione fornisce indicazioni generali per configurare e testare un'implementazione di AWS WAF Bot Control per il tuo sito. I passaggi specifici che sceglierai di seguire dipenderanno dalle tue esigenze, dalle tue risorse e dalle richieste web che ricevi.

Queste informazioni si aggiungono alle informazioni generali su test e ottimizzazione fornite all'indirizzoTest e ottimizzazione delle protezioni AWS WAF.

> **Note**
>
> AWS Le Managed Rules sono progettate per proteggerti dalle minacce web più comuni. Se utilizzati in conformità con la documentazione, i gruppi di regole AWS Managed Rules aggiungono un altro livello di sicurezza per le applicazioni. Tuttavia, i gruppi di regole AWS Managed Rules non sono intesi come sostituti delle responsabilità in materia di sicurezza, che sono determinate dalle AWS risorse selezionate. Fai riferimento al modello di responsabilità condivisa per assicurarti che le tue risorse AWS siano adeguatamente protette.

> **Rischio legato al traffico di produzione**
>
> Prima di implementare l'implementazione di Bot Control per il traffico di produzione, testala e ottimizzala in un ambiente di staging o test finché non ti senti a tuo agio con il potenziale impatto sul traffico. Quindi testa e ottimizza le regole in modalità di conteggio in base al traffico di produzione prima di attivarle.

Questa guida è destinata agli utenti che in generale sanno come creare e gestire ACL AWS WAF Web, regole e gruppi di regole. Questi argomenti sono trattati nelle sezioni precedenti di questa guida.

Per configurare e testare un'implementazione di Bot Control

Esegui questi passaggi prima in un ambiente di test, poi in produzione.

1. Aggiungi il gruppo di regole gestito da Bot Control

> **Note**
>
> Ti vengono addebitati costi aggiuntivi quando utilizzi questo gruppo di regole gestito. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

Aggiungi il gruppo di AWS regole gestito `AWSManagedRulesBotControlRuleSet` a un ACL web nuovo o esistente e configuralo in modo che non alteri il comportamento corrente dell'ACL web.

- Quando aggiungi il gruppo di regole gestito, modificalo e procedi come segue:
  - Nel riquadro Livello di ispezione, seleziona il livello di ispezione che desideri utilizzare.
    - Comune: rileva una varietà di bot che si identificano automaticamente, come framework di web scraping, motori di ricerca e browser automatici. Le protezioni Bot Control a questo livello identificano i bot più comuni utilizzando tecniche di rilevamento dei bot tradizionali, come l'analisi statica dei dati delle richieste. Le regole etichettano il traffico proveniente da questi bot e bloccano quello che non possono verificare.
    - Mirato: include le protezioni di livello comune e aggiunge il rilevamento mirato per bot sofisticati che non si identificano automaticamente. Le protezioni mirate mitigano l'attività dei bot utilizzando una combinazione di limitazioni della velocità e sfide legate al CAPTCHA e al browser in background.
      - **`TGT_`**— Le regole che forniscono una protezione mirata hanno nomi che iniziano con. `TGT_` Tutte le protezioni mirate utilizzano tecniche di rilevamento come l'interrogazione del browser, il rilevamento delle impronte digitali e l'euristica comportamentale per identificare il traffico di bot non valido.
      - **`TGT_ML_`**— Le regole di protezione mirate che utilizzano l'apprendimento automatico hanno nomi che iniziano con. `TGT_ML_` Queste regole utilizzano l'analisi automatizzata e basata sull'apprendimento automatico delle statistiche sul traffico dei siti Web per rilevare comportamenti anomali indicativi di un'attività distribuita e coordinata dei bot. AWS WAF analizza le statistiche sul traffico del sito Web, ad esempio timestamp, caratteristiche del browser e URL visitato in precedenza, per migliorare il modello di apprendimento automatico di Bot Control. Le funzionalità di machine learning sono abilitate per impostazione predefinita, ma puoi disabilitarle nella configurazione del

gruppo di regole. Quando l'apprendimento automatico è disabilitato, AWS WAF non valuta queste regole.

Per ulteriori informazioni su questa scelta, vedereAWS WAF Gruppo di regole Bot Control.

- Nel riquadro Regole, apri il menu a discesa Sostituisci tutte le azioni delle regole e scegli. Count Con questa configurazione, AWS WAF valuta le richieste in base a tutte le regole del gruppo di regole e conta solo le corrispondenze risultanti, pur continuando ad aggiungere etichette alle richieste. Per ulteriori informazioni, consulta Sovrascrivere le azioni delle regole in un gruppo di regole.

  Con questo override, puoi monitorare il potenziale impatto delle regole di Bot Control sul tuo traffico, per determinare se desideri aggiungere eccezioni per cose come casi d'uso interni o bot desiderati.

- Posiziona il gruppo di regole in modo che venga valutato per ultimo nell'ACL Web, con un'impostazione di priorità numericamente più alta rispetto a qualsiasi altra regola o gruppo di regole che stai già utilizzando. Per ulteriori informazioni, consulta Ordine di elaborazione delle regole e dei gruppi di regole in un ACL Web.

  In questo modo, la tua attuale gestione del traffico non viene interrotta. Ad esempio, se disponi di regole che rilevano traffico dannoso come SQL injection o cross-site scripting, continueranno a rilevare e registrare tali richieste. In alternativa, se disponi di regole che consentono il traffico noto e non dannoso, possono continuare a consentire tale traffico senza che venga bloccato dal gruppo di regole gestito da Bot Control. Potresti decidere di modificare l'ordine di elaborazione durante le attività di test e ottimizzazione, ma questo è un buon modo per iniziare.

2. Abilita il campionamento, la registrazione e le metriche per l'ACL Web

   Se necessario, configura la registrazione per l'ACL Web e abilita il campionamento e i parametri Amazon. CloudWatch Puoi utilizzare le metriche e la registrazione per monitorare l'interazione del tuo traffico web con il gruppo di regole gestito da Bot Control.

   - Per informazioni sulla configurazione e l'utilizzo della registrazione, consulta. Registrazione del traffico AWS WAF ACL Web
   - Per informazioni sui CloudWatch parametri di Amazon, consultaMonitoraggio con Amazon CloudWatch.
   - Per informazioni sul campionamento delle richieste web, consulta. Visualizzazione di un esempio di richieste Web

3. Associare l'ACL Web a una risorsa

   Se l'ACL Web non è già associato a una risorsa, associala. Per informazioni, consulta Associazione o dissociazione di un ACL Web con una risorsa AWS.

4. Monitora il traffico e la corrispondenza delle regole di Bot Control

   Assicurati che il traffico scorra e che le regole del gruppo di regole gestito da Bot Control aggiungano etichette alle richieste web corrispondenti. Puoi vedere le etichette nei log e vedere le metriche dei bot e delle etichette nei parametri di Amazon CloudWatch . Nei log, le regole che hai sostituito per conteggiare nel gruppo di regole vengono visualizzate in `ruleGroupList` with `action` set to count e `overriddenAction` indicano l'azione della regola configurata che hai ignorato.

   > **Note**
   >
   > Il gruppo di regole gestito da Bot Control verifica i bot utilizzando gli indirizzi IP di. AWS WAF Se utilizzi Bot Control e hai verificato i bot che effettuano il routing attraverso un proxy o un sistema di bilanciamento del carico, potresti dover autorizzarli esplicitamente utilizzando una regola personalizzata. Per informazioni su come creare una regola personalizzata, consulta. Indirizzo IP inoltrato Per informazioni su come utilizzare la regola per personalizzare la gestione delle richieste web di Bot Control, consulta il passaggio successivo.

   Esamina attentamente la gestione delle richieste web per individuare eventuali falsi positivi che potresti dover mitigare con una gestione personalizzata. Per esempi di falsi positivi, vedere. Falsi positivi con AWS WAF Bot Control

5. Personalizza la gestione delle richieste web di Bot Control

   Se necessario, aggiungi le tue regole che consentono o bloccano esplicitamente le richieste, per modificare il modo in cui le regole di Bot Control le gestirebbero altrimenti.

   Il modo in cui eseguire questa operazione dipende dal caso d'uso, ma le soluzioni più comuni sono le seguenti:

   - Consenti esplicitamente le richieste con una regola che aggiungi prima del gruppo di regole gestito da Bot Control. In questo modo, le richieste consentite non raggiungono mai il gruppo

di regole per la valutazione. Questo può aiutare a contenere il costo dell'utilizzo del gruppo di regole gestito da Bot Control.

- Escludi le richieste dalla valutazione di Bot Control aggiungendo un'istruzione scope-down all'interno dell'istruzione del gruppo di regole gestito da Bot Control. Funziona come l'opzione precedente. Può aiutare a contenere i costi dell'utilizzo del gruppo di regole gestito da Bot Control, poiché le richieste che non corrispondono all'istruzione scope-down non raggiungono mai la valutazione del gruppo di regole. Per informazioni sulle istruzioni scope-down, consulta. Dichiarazioni delimitate

  Per esempi di , consulta le sezioni seguenti:

  - Escludi l'intervallo IP dalla gestione dei bot
  - Consenti il traffico proveniente da un bot che controlli
- Utilizza le etichette Bot Control nella gestione delle richieste per consentire o bloccare le richieste. Aggiungi una regola di corrispondenza delle etichette dopo il gruppo di regole gestito da Bot Control per filtrare le richieste etichettate che desideri consentire da quelle che desideri bloccare.

  Dopo il test, mantieni le relative regole di Bot Control in modalità count e mantieni le decisioni sulla gestione delle richieste nella tua regola personalizzata. Per informazioni sulle istruzioni label match, consultaDichiarazione della regola di corrispondenza delle etichette.

  Per esempi di questo tipo di personalizzazione, consulta quanto segue:

  - Crea un'eccezione per un agente utente bloccato
  - Consenti uno specifico bot bloccato
  - Blocca i bot verificati

Per ulteriori esempi, consulta AWS WAF Esempi di Bot Control.

6. Se necessario, abilita le impostazioni del gruppo di regole gestito da Bot Control

   A seconda della situazione, potresti aver deciso di lasciare alcune regole di Bot Control in modalità count o con un'azione diversa. Per le regole che desideri far eseguire così come sono configurate all'interno del gruppo di regole, abilita la normale configurazione delle regole. A tale scopo, modifica l'istruzione del gruppo di regole nell'ACL Web e apporta le modifiche nel riquadro Regole.

AWS WAF Esempi di Bot Control

Questa sezione mostra configurazioni di esempio che soddisfano una serie di casi d'uso comuni per le implementazioni di AWS WAF Bot Control.

Ogni esempio fornisce una descrizione del caso d'uso e quindi mostra la soluzione negli elenchi JSON per le regole configurate personalizzate.

> **Note**
>
> Gli elenchi JSON mostrati in questi esempi sono stati creati nella console configurando la regola e quindi modificandola utilizzando l'editor Rule JSON.

Argomenti

Esempio di Bot Control: configurazione semplice

Il seguente elenco JSON mostra un esempio di ACL web con un gruppo di regole gestito da AWS WAF Bot Control. Nota la configurazione di visibilità, che consente di AWS WAF archiviare gli esempi e le metriche delle richieste per scopi di monitoraggio.

```
{
  "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
}
```

Esempio di controllo dei bot: consenti esplicitamente i bot verificati

AWS WAF Bot Control non blocca i bot noti AWS per essere bot comuni e verificabili. Quando Bot Control identifica una richiesta web come proveniente da un bot verificato, aggiunge un'etichetta che nomina il bot e un'etichetta che indica che si tratta di un bot verificato. Bot Control non aggiunge altre etichette, come le etichette dei segnali, per evitare che i bot noti come validi vengano bloccati.

Potresti avere altre AWS WAF regole che bloccano i bot verificati. Se vuoi assicurarti che i bot verificati siano consentiti, aggiungi una regola personalizzata per consentirli in base alle etichette Bot Control. La tua nuova regola deve seguire il gruppo di regole gestito da Bot Control, in modo che le etichette siano disponibili per il confronto.

La seguente regola consente esplicitamente i bot verificati.

```
{
    "Name": "match_rule",
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
      "Allow": {}
    }
}
```

Esempio di controllo dei bot: blocca i bot verificati

Per bloccare i bot verificati, devi aggiungere una regola per bloccarli che segue il gruppo di regole gestito da AWS WAF Bot Control. A tale scopo, identifica i nomi dei bot che desideri bloccare e utilizza un'istruzione label match per identificarli e bloccarli. Se vuoi bloccare solo tutti i bot verificati, puoi omettere la corrispondenza con l'`bot:name:`etichetta.

La seguente regola blocca solo il bot `bingbot` verificato. Questa regola deve essere eseguita dopo il gruppo di regole gestito da Bot Control.

```
{
    "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 seguente regola blocca tutti i bot verificati.

```
{
    "Name": "match_rule",
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    }
}
```

Esempio di Bot Control: consenti uno specifico bot bloccato

È possibile che un bot venga bloccato da più di una delle regole di Bot Control. Esegui la procedura seguente per ogni regola di blocco.

Se una regola di AWS WAF Bot Control blocca un bot che non desideri bloccare, procedi come segue:

1. Identifica la regola Bot Control che blocca il bot controllando i log. La regola di blocco verrà specificata nei log nei campi i cui nomi iniziano con. `terminatingRule` Per informazioni sui registri ACL Web, vedere. Registrazione del traffico AWS WAF ACL Web Nota l'etichetta che la regola aggiunge alle richieste.
2. Nell'ACL Web, sostituisci l'azione della regola di blocco per eseguire il conteggio. Per eseguire questa operazione nella console, modifica la regola del gruppo di regole nell'ACL Web e scegli un'azione che sostituisca l'azione della Count regola per la regola. Ciò garantisce che il bot non venga bloccato dalla regola, ma la regola applicherà comunque la sua etichetta alle richieste corrispondenti.
3. Aggiungi una regola di corrispondenza delle etichette all'ACL web, dopo il gruppo di regole gestito da Bot Control. Configura la regola in modo che corrisponda all'etichetta della regola sostituita e per bloccare tutte le richieste corrispondenti ad eccezione del bot che non desideri bloccare.

   Il tuo ACL web è ora configurato in modo che il bot che desideri consentire non sia più bloccato dalla regola di blocco che hai identificato nei log.

Controlla nuovamente il traffico e i log per assicurarti che al bot sia consentito l'accesso. In caso contrario, esegui nuovamente la procedura precedente.

Ad esempio, supponiamo di voler bloccare tutti i bot di monitoraggio tranne. `pingdom` In questo caso, sostituite la `CategoryMonitoring` regola di conteggio e quindi scrivete una regola per bloccare tutti i bot di monitoraggio ad eccezione di quelli con l'etichetta del nome del bot. `pingdom`

La regola seguente utilizza il gruppo di regole gestito da Bot Control ma sostituisce l'azione della regola per contare. `CategoryMonitoring` La regola di monitoraggio delle categorie applica le sue etichette come di consueto alle richieste corrispondenti, ma le conta solo invece di eseguire la consueta azione di blocco.

```
{
  "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 regola seguente corrisponde all'etichetta di monitoraggio della categoria che la `CategoryMonitoring` regola precedente aggiunge alle richieste Web corrispondenti. Tra le richieste di monitoraggio delle categorie, questa regola blocca tutte tranne quelle che hanno un'etichetta per il nome `pingdom` del bot.

La seguente regola deve essere eseguita dopo il precedente gruppo di regole gestito da Bot Control nell'ordine di elaborazione 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"
      }
}
```

Esempio di Bot Control: crea un'eccezione per un agente utente bloccato

Se il traffico proveniente da alcuni user agent diversi dal browser viene bloccato erroneamente, puoi creare un'eccezione impostando la regola AWS WAF Bot Control non valida su Count e combinando quindi l'etichettatura della regola `SignalNonBrowserUserAgent` con i criteri di eccezione impostati.

> **Note**
>
> Le app per dispositivi mobili in genere hanno agenti utente diversi dal browser, che la regola blocca per impostazione predefinita. `SignalNonBrowserUserAgent`

La regola seguente utilizza il gruppo di regole gestito da Bot Control ma sostituisce l'azione della regola per `SignalNonBrowserUserAgent` Count. La regola del segnale applica le sue etichette come di consueto alle richieste corrispondenti, ma le conta solo invece di eseguire la consueta azione di blocco.

```
{
  "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 seguente regola corrisponde all'etichetta del segnale che la `SignalNonBrowserUserAgent` regola Bot Control aggiunge alle richieste web corrispondenti. Tra le richieste di segnale, questa regola blocca tutte tranne quelle che hanno lo user agent che vogliamo consentire.

La seguente regola deve essere eseguita dopo il precedente gruppo di regole gestito da Bot Control nell'ordine di elaborazione 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"
    }
}
```

Esempio di Bot Control: usa Bot Control solo per la pagina di accesso

L'esempio seguente utilizza un'istruzione scope-down per applicare AWS WAF Bot Control solo al traffico che arriva alla pagina di accesso di un sito Web, identificata dal percorso URI. `login` Il percorso URI della pagina di accesso potrebbe essere diverso da quello dell'esempio, a seconda dell'applicazione e dell'ambiente.

```
{
  "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"
      }
```

```
    }
  }
}
```

Esempio di Bot Control: utilizza Bot Control solo per contenuti dinamici

Questo esempio utilizza un'istruzione scope-down per applicare AWS WAF Bot Control solo al contenuto dinamico.

L'istruzione scope-down esclude il contenuto statico annullando i risultati della corrispondenza per un set di pattern regex:

- Il set di pattern regex è configurato per corrispondere alle estensioni del contenuto statico. Ad esempio, la specifica del set di pattern regex potrebbe essere. `(?i)\.(jpe?g|gif|png|svg|ico|css|js|woff2?)$` Per informazioni sui set e sulle istruzioni di pattern regex, vedere. Istruzione regola di corrispondenza del set del modello regex
- Nell'istruzione scope-down, escludiamo il contenuto statico corrispondente annidando l'istruzione regex pattern set all'interno di un'istruzione. `NOT` Per informazioni sulla dichiarazione, vedere. `NOT` NOTdichiarazione delle regole

```
{
  "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"
              }
            ]
          }
        }
      }
    }
  }
}
```

Esempio di controllo dei bot: esclusione dell'intervallo IP dalla gestione dei bot

Se desideri escludere un sottoinsieme di traffico web dalla gestione di AWS WAF Bot Control e puoi identificare quel sottoinsieme utilizzando un'istruzione di regola, escludilo aggiungendo un'istruzione scope-down all'istruzione del gruppo di regole gestita da Bot Control.

La seguente regola esegue la normale gestione dei bot di Bot Control su tutto il traffico Web, ad eccezione delle richieste Web provenienti da un intervallo di indirizzi IP specifico.

```
{
  "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"
          }
        }
      }
    }
  }
}
```

Esempio di controllo dei bot: consenti il traffico proveniente da un bot che controlli

Puoi configurare alcuni bot di monitoraggio del sito e bot personalizzati per inviare intestazioni personalizzate. Se desideri consentire il traffico proveniente da questi tipi di bot, puoi configurarli per aggiungere un segreto condiviso in un'intestazione. Puoi quindi escludere i messaggi con l'intestazione aggiungendo un'istruzione scope-down all'istruzione del gruppo di regole gestito da AWS WAF Bot Control.

La seguente regola di esempio esclude il traffico con un'intestazione segreta dall'ispezione di Bot Control.

```
{
  "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"
          }
        }
      }
    }
  }
```

Esempio di Bot Control: livello di ispezione mirato

Per un livello di protezione avanzato, puoi abilitare il livello di ispezione mirata nel gruppo di regole gestito da AWS WAF Bot Control.

Nell'esempio seguente, le funzionalità di machine learning sono abilitate. È possibile disattivare questo comportamento impostando `EnableMachineLearning` su`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"
    }
  }
}
```

Esempio di Bot Control: utilizza due istruzioni per limitare l'uso del livello di ispezione mirato

Per ottimizzare i costi, puoi utilizzare due istruzioni del gruppo di regole gestite da AWS WAF Bot Control nell'ACL web, con livelli e ambiti di ispezione separati. Ad esempio, è possibile estendere l'istruzione Targeted Inspection Level solo agli endpoint applicativi più sensibili.

Le due istruzioni nell'esempio seguente hanno un ambito che si esclude a vicenda. Senza questa configurazione, una richiesta potrebbe comportare due valutazioni fatturate.

> **Note**
>
> Il riferimento a più istruzioni `AWSManagedRulesBotControlRuleSet` non è supportato nell'editor visivo della console. Utilizza invece l'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 integrazione delle applicazioni client

Utilizza le API di integrazione delle applicazioni AWS WAF client per abbinare le protezioni lato client alle protezioni ACL Web AWS lato server, per verificare che le applicazioni client che inviano richieste Web alle risorse protette siano i client previsti e che gli utenti finali siano esseri umani.

Utilizza le integrazioni client per gestire le sfide silenziose del browser e i puzzle CAPTCHA, ottenere token con prove del successo del browser e delle risposte degli utenti finali e includere questi token nelle richieste agli endpoint protetti. Per informazioni generali sui token, consulta. AWS WAF AWS WAF token di richiesta web

Combina le integrazioni con i client con le protezioni Web ACL che richiedono token validi per l'accesso alle tue risorse. Puoi utilizzare gruppi di regole che controllano e monitorano i token di sfida, come quelli elencati nella sezione successiva, all'indirizzoIntegrazione intelligente delle minacce e regole AWS gestite, e puoi utilizzare le azioni e le Challenge regole per controllare, come descritto in. CAPTCHA CAPTCHAe Challenge in AWS WAF

AWS WAF offre due livelli di integrazione per JavaScript le applicazioni e uno per le applicazioni mobili:

- Integrazione intelligente delle minacce: verifica l'applicazione client e fornisci l'acquisizione e la gestione dei AWS token. Questa funzionalità è simile alla funzionalità fornita dall'azione della AWS WAF Challenge regola. Questa funzionalità integra completamente l'applicazione client con il gruppo di regole `AWSManagedRulesACFPRuleSet` gestito, il gruppo di regole `AWSManagedRulesATPRuleSet` gestito e il livello di protezione mirato del gruppo di regole `AWSManagedRulesBotControlRuleSet` gestito.

  Le API intelligenti per l'integrazione delle minacce utilizzano la tecnologia AWS WAF Silent Browser Challenge per garantire che i tentativi di accesso e le altre chiamate alla risorsa protetta siano consentiti solo dopo che il client ha acquisito un token valido. Le API gestiscono l'autorizzazione dei token per le sessioni dell'applicazione client e raccolgono informazioni sul client per determinare se è gestito da un bot o da un essere umano.

  > **Note**
  >
  > È disponibile per JavaScript e per le applicazioni mobili Android e iOS.

- Integrazione CAPTCHA: verifica gli utenti finali con un puzzle CAPTCHA personalizzato che gestisci nella tua applicazione. È simile alla funzionalità fornita dall'azione della AWS WAF CAPTCHA regola, ma con un maggiore controllo sul posizionamento e sul comportamento del puzzle.

  Questa integrazione sfrutta l'integrazione JavaScript intelligente delle minacce per eseguire sfide silenziose e fornire AWS WAF token alla pagina del cliente.

  > **Note**
  >
  > È disponibile per JavaScript le applicazioni.

Argomenti

- Integrazione intelligente delle minacce e regole AWS gestite
- Accesso alle API di integrazione
- AWS WAF JavaScript integrazioni

- AWS WAF integrazione di applicazioni mobili

Integrazione intelligente delle minacce e regole AWS gestite

Le API di integrazione intelligente delle minacce funzionano con gli ACL Web che utilizzano i gruppi di regole intelligenti sulle minacce per abilitare la piena funzionalità di questi gruppi di regole gestiti avanzati.

- AWS WAF Gruppo di regole gestito per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control. `AWSManagedRulesACFPRuleSet`

  La frode nella creazione di account è un'attività illegale online in cui un utente malintenzionato crea account non validi nell'applicazione per scopi quali ricevere bonus di iscrizione o spacciarsi per qualcuno. Il gruppo di regole gestito da ACFP fornisce regole per bloccare, etichettare e gestire le richieste che potrebbero far parte di tentativi fraudolenti di creazione di account. Le API consentono di ottimizzare la verifica del browser del client e le informazioni sull'interattività umana che le regole ACFP utilizzano per separare il traffico client valido dal traffico dannoso.

  Per ulteriori informazioni, consultare AWS WAF Gruppo di regole per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control e AWS WAF Fraud Control creazione di account e prevenzione delle frodi (ACFP).
- AWS WAF Gruppo di regole gestito per la prevenzione dell'acquisizione di account Fraud Control (ATP). `AWSManagedRulesATPRuleSet`

  L'acquisizione di un account è un'attività illegale online in cui un utente malintenzionato ottiene l'accesso non autorizzato all'account di una persona. Il gruppo di regole gestito dall'ATP fornisce regole per bloccare, etichettare e gestire le richieste che potrebbero far parte di tentativi malevoli di acquisizione di account. Le API consentono la verifica precisa dei client e l'aggregazione del comportamento che le regole ATP utilizzano per separare il traffico client valido dal traffico dannoso.

  Per ulteriori informazioni, consultare AWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi e AWS WAF Controllo delle frodi e prevenzione delle acquisizioni di conti (ATP).
- Livello di protezione mirato del gruppo di regole gestito da Bot Control AWS WAF . `AWSManagedRulesBotControlRuleSet`

I bot vanno da quelli utili e che si identificano da soli, come la maggior parte dei motori di ricerca e dei crawler, ai bot dannosi che agiscono contro il tuo sito web e non si identificano da soli. Il gruppo di regole gestito da Bot Control fornisce regole per monitorare, etichettare e gestire l'attività dei bot nel traffico web. Quando si utilizza il livello di protezione mirato di questo gruppo di regole, le regole mirate utilizzano le informazioni sulla sessione client fornite dalle API per rilevare meglio i bot dannosi.

Per ulteriori informazioni, consultare AWS WAF Gruppo di regole Bot Control e AWS WAF Controllo dei bot.

Per aggiungere uno di questi gruppi di regole gestiti all'ACL Web, consulta le procedure Aggiungere il gruppo di regole gestite ACFP all'ACL Web e. Aggiungere il gruppo di regole gestite da ATP all'ACL Web Aggiungere il gruppo di regole gestito da AWS WAF Bot Control all'ACL web

> **Note**
>
> I gruppi di regole gestiti attualmente non bloccano le richieste che contengono token mancanti. Per bloccare le richieste contenenti token mancanti, dopo aver implementato le API di integrazione delle applicazioni, segui le istruzioni riportate all'indirizzo. Bloccare le richieste che non hanno un token valido

Accesso alle API di integrazione

Le API di JavaScript integrazione sono generalmente disponibili e puoi utilizzarle per i tuoi browser e altri dispositivi che eseguono JavaScript.

AWS WAF offre SDK personalizzati per l'integrazione intelligente delle minacce per app mobili Android e iOS.

- Per le app mobili Android, gli AWS WAF SDK funzionano con l'API Android versione 23 (Android versione 6) e successive. Per informazioni sulle versioni di Android, consulta le note di rilascio della piattaforma SDK.
- Per le app mobili iOS, AWS WAF gli SDK funzionano per iOS versione 13 e successive. Per informazioni sulle versioni di iOS, consulta le note di rilascio di iOS e iPadOS.

Per accedere alle API di integrazione tramite la console

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Scegli Integrazione delle applicazioni nel riquadro di navigazione, quindi scegli la scheda che ti interessa.

   - L'integrazione intelligente delle minacce è disponibile per JavaScript tutte le applicazioni mobili.

     La scheda contiene quanto segue:

     - Un elenco degli ACL Web abilitati per l'integrazione intelligente delle applicazioni contro le minacce. L'elenco include ogni ACL Web che utilizza il gruppo di regole `AWSManagedRulesACFPRuleSet` gestito, il gruppo di regole `AWSManagedRulesATPRuleSet` gestite o il livello di protezione mirato del gruppo di regole `AWSManagedRulesBotControlRuleSet` gestito. Quando si implementano le API intelligenti per le minacce, si utilizza l'URL di integrazione per l'ACL Web con cui si desidera effettuare l'integrazione.
     - Le API a cui hai accesso. Le JavaScript API sono sempre disponibili. Per accedere agli SDK per dispositivi mobili, contatta l'assistenza all'indirizzo Contact. AWS
   - L'integrazione CAPTCHA è disponibile per le applicazioni. JavaScript

     La scheda contiene quanto segue:

     - L'URL di integrazione da utilizzare nella tua integrazione.
     - Le chiavi API che hai creato per i domini delle tue applicazioni client. L'utilizzo dell'API CAPTCHA richiede una chiave API crittografata che dia ai clienti il diritto di accedere al AWS WAF CAPTCHA dai loro domini. Per ogni client con cui effettui l'integrazione, utilizza una chiave API che contenga il dominio del client. Per ulteriori informazioni su questi requisiti e sulla gestione di queste chiavi, consultaGestione delle chiavi API per l'API JS CAPTCHA.

AWS WAF JavaScript integrazioni

Puoi utilizzare le API di JavaScript integrazione per implementare integrazioni di AWS WAF applicazioni nei tuoi browser e in altri dispositivi che eseguono. JavaScript

- Le API intelligenti per le minacce consentono di gestire l'autorizzazione dei token tramite una sfida silenziosa sul browser lato client e di includere i token nelle richieste inviate alle risorse protette.

- L'API di integrazione CAPTCHA si aggiunge alle API intelligenti per le minacce e consente di personalizzare il posizionamento e le caratteristiche del puzzle CAPTCHA nelle applicazioni client. Questa API sfrutta le API intelligenti per le minacce per acquisire AWS WAF token da utilizzare nella pagina dopo che l'utente finale ha completato con successo il puzzle CAPTCHA.

Utilizzando queste integrazioni, ti assicuri che le chiamate di procedura remota del tuo client contengano un token valido. Quando queste API di integrazione sono presenti nelle pagine dell'applicazione, puoi implementare regole di mitigazione nell'ACL web, come bloccare le richieste che non contengono un token valido. Puoi anche implementare regole che impongono l'uso dei token ottenuti dalle tue applicazioni client, utilizzando le azioni Challenge o CAPTCHA nelle tue regole.

L'elenco seguente mostra i componenti di base di un'implementazione tipica delle API per le minacce intelligenti in una pagina di applicazione 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>
```

L'API di integrazione CAPTCHA consente di personalizzare l'esperienza con i puzzle CAPTCHA degli utenti finali. L'integrazione CAPTCHA sfrutta l'integrazione JavaScript intelligente delle minacce, per la verifica del browser e la gestione dei token, e aggiunge una funzione per la configurazione e il rendering del puzzle CAPTCHA.

L'elenco seguente mostra i componenti di base di un'implementazione tipica dell'API JavaScript CAPTCHA in una pagina di applicazione 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>
```

Argomenti

- Fornire domini da utilizzare nei token
- Utilizzo dell' JavaScript API con politiche di sicurezza dei contenuti
- Utilizzo dell' JavaScript API per le minacce intelligenti
- Utilizzo dell'API CAPTCHA JavaScript

Fornire domini da utilizzare nei token

Per impostazione predefinita, quando AWS WAF crea un token, utilizza il dominio host della risorsa associata all'ACL web. Puoi fornire domini aggiuntivi per i token AWS WAF creati per le API.

JavaScript Per fare ciò, configura la variabile globale`window.awsWafCookieDomainList`, con uno o più domini token.

Quando AWS WAF crea un token, utilizza il dominio più appropriato e più breve tra la combinazione dei domini `window.awsWafCookieDomainList` e del dominio host della risorsa associata all'ACL web.

Impostazioni di esempio:

```
window.awsWafCookieDomainList = ['.aws.amazon.com']
```

```
window.awsWafCookieDomainList = ['.aws.amazon.com', 'abc.aws.amazon.com']
```

Non puoi usare suffissi pubblici in questo elenco. Ad esempio, non puoi utilizzare `gov.au` or `co.uk` come domini token nell'elenco.

I domini specificati in questo elenco devono essere compatibili con gli altri domini e configurazioni di dominio:

- I domini devono essere accettabili, in base al dominio host protetto e all'elenco di domini token configurato per l'ACL web. AWS WAF Per ulteriori informazioni, consulta Configurazione dell'elenco dei domini del token ACL Web.
- Se utilizzi l'API JavaScript CAPTCHA, almeno un dominio nella tua chiave API CAPTCHA deve corrispondere esattamente a uno dei domini token in `window.awsWafCookieDomainList` o deve essere il dominio apex di uno di quei domini token.

  Ad esempio, per il dominio token`mySubdomain.myApex.com`, la chiave API corrisponde esattamente e la chiave API `mySubdomain.myApex.com` è il dominio apex. `myApex.com` Entrambe le chiavi corrispondono al dominio del token.

  Per ulteriori informazioni sulle chiavi API, consultaGestione delle chiavi API per l'API JS CAPTCHA.

Se utilizzi il gruppo di regole `AWSManagedRulesACFPRuleSet` gestito, potresti configurare un dominio che corrisponda a quello nel percorso di creazione dell'account che hai fornito per la configurazione del gruppo di regole. Per ulteriori informazioni su questa configurazione, consulta Aggiungere il gruppo di regole gestite ACFP all'ACL Web.

Se utilizzi il gruppo di regole `AWSManagedRulesATPRuleSet` gestito, potresti configurare un dominio che corrisponda a quello nel percorso di accesso che hai fornito alla configurazione del gruppo di regole. Per ulteriori informazioni su questa configurazione, consulta Aggiungere il gruppo di regole gestite da ATP all'ACL Web.

Utilizzo dell' JavaScript API con politiche di sicurezza dei contenuti

Se applichi politiche di sicurezza dei contenuti (CSP) alle tue risorse, affinché JavaScript l'implementazione funzioni, devi inserire nella lista consentita il dominio AWS WAF apex. `awswaf.com` Gli JavaScript SDK effettuano chiamate a diversi AWS WAF endpoint, quindi l'allowlisting di questo dominio fornisce le autorizzazioni necessarie agli SDK per funzionare.

Di seguito viene mostrato un esempio di configurazione per inserire nella lista consentita il dominio apex: AWS WAF

```
connect-src 'self' https://*.awswaf.com;
script-src 'self' https://*.awswaf.com;
script-src-elem 'self' https://*.awswaf.com;
```

Se provi a utilizzare gli JavaScript SDK con risorse che utilizzano CSP e non hai inserito il AWS WAF dominio nella lista consentita, riceverai errori come i seguenti:

```
Refused to load the script ...awswaf.com/<> because it violates the following Content
 Security Policy directive: “script-src ‘self’
```

Utilizzo dell' JavaScript API per le minacce intelligenti

Le API intelligenti per le minacce forniscono operazioni per l'esecuzione di sfide silenziose sul browser dell'utente e per la gestione dei AWS WAF token che forniscono la prova dell'avvenuta riuscita della sfida e delle risposte CAPTCHA.

Implementa l' JavaScript integrazione prima in un ambiente di test, poi in produzione. Per ulteriori indicazioni sulla codifica, consulta le sezioni seguenti.

Per utilizzare le API intelligenti per le minacce

1. Installa le API

   Se utilizzi l'API CAPTCHA, puoi saltare questo passaggio. Quando installi l'API CAPTCHA, lo script installa automaticamente le API intelligenti per le minacce.

a. Accedi AWS Management Console e apri la console all'indirizzo https://console.aws.amazon.com/wafv2/. AWS WAF

b. Nel riquadro di navigazione, scegliere Application integration (Integrazione di applicazioni). Nella pagina di integrazione dell'applicazione, puoi vedere le opzioni a schede.

c. Seleziona Integrazione intelligente delle minacce

d. Nella scheda, seleziona l'ACL web con cui desideri effettuare l'integrazione. L'elenco degli ACL Web include solo gli ACL Web che utilizzano il gruppo di regole `AWSManagedRulesACFPRuleSet` gestito, il gruppo di regole `AWSManagedRulesATPRuleSet` gestite o il livello di protezione mirato del gruppo di regole `AWSManagedRulesBotControlRuleSet` gestito.

e. Apri il riquadro JavaScript SDK e copia il tag script per utilizzarlo nella tua integrazione.

f. Nel codice della pagina dell'applicazione, nella `<head>` sezione, inserisci il tag script che hai copiato per l'ACL web. Questa inclusione fa sì che l'applicazione client recuperi automaticamente un token in background al caricamento della pagina.

```
<head>
    <script type="text/javascript" src="Web ACL integration URL/challenge.js”
 defer></script>
<head>
```

Questo `<script>` elenco è configurato con l'`defer`attributo, ma puoi modificare l'impostazione `async` se desideri un comportamento diverso per la tua pagina.

2. (Facoltativo) Aggiungi la configurazione del dominio per i token del client: per impostazione predefinita, quando viene AWS WAF creato un token, questo utilizza il dominio host della risorsa associata all'ACL web. Per fornire domini aggiuntivi per le JavaScript API, segui le indicazioni all'indirizzo. Fornire domini da utilizzare nei token

3. Codifica la tua integrazione intelligente contro le minacce: scrivi il codice per assicurarti che il recupero dei token venga completato prima che il client invii le sue richieste agli endpoint protetti. Se stai già utilizzando l'`fetch`API per effettuare la chiamata, puoi sostituire il wrapper di integrazione. AWS WAF `fetch` Se non utilizzi l'`fetch`API, puoi invece utilizzare l'operazione di AWS WAF integrazione`getToken`. Per indicazioni sulla codifica, consulta le seguenti sezioni.

4. Aggiungi la verifica tramite token nell'ACL Web: aggiungi almeno una regola all'ACL Web che verifichi la presenza di un token di sfida valido nelle richieste Web inviate dal client. Puoi utilizzare gruppi di regole che controllano e monitorano i token di sfida, come il livello mirato

del gruppo di regole gestito da Bot Control, e puoi utilizzare l'azione delle Challenge regole per verificare, come descritto in. CAPTCHAe Challenge in AWS WAF

Le aggiunte Web ACL verificano che le richieste ai tuoi endpoint protetti includano il token che hai acquisito nell'integrazione con il client. Le richieste che includono un token valido e non scaduto superano l'Challengeispezione e non inviano un'altra sfida silenziosa al cliente.

5. (Facoltativo) Blocca le richieste con token mancanti: se utilizzi le API con il gruppo di regole gestito ACFP, il gruppo di regole gestito ATP o le regole mirate del gruppo di regole Bot Control, queste regole non bloccano le richieste che contengono token mancanti. Per bloccare le richieste che contengono token mancanti, segui le istruzioni riportate all'indirizzo. Bloccare le richieste che non hanno un token valido

Argomenti

- Specifiche dell'API per le minacce intelligenti
- Come usare il fetch wrapper di integrazione
- Come usare l'integrazione getToken

Specifiche dell'API per le minacce intelligenti

Questa sezione elenca le specifiche per i metodi e le proprietà delle JavaScript API intelligenti di mitigazione delle minacce. Utilizza queste API per le integrazioni intelligenti di minacce e CAPTCHA.

`AwsWafIntegration.fetch()`

Invia la `fetch` richiesta HTTP al server utilizzando l'implementazione dell'integrazione. AWS WAF

`AwsWafIntegration.getToken()`

Recupera il AWS WAF token memorizzato e lo memorizza in un cookie nella pagina corrente con il nome `aws-waf-token` e il valore impostato sul valore del token.

`AwsWafIntegration.hasToken()`

Restituisce un valore booleano che indica se il `aws-waf-token` cookie contiene attualmente un token non scaduto.

Se utilizzi anche l'integrazione CAPTCHA, consulta le relative specifiche all'indirizzo. Specifiche dell'API CAPTCHA JavaScript

Come usare il **`fetch`** wrapper di integrazione

È possibile utilizzare il AWS WAF `fetch` wrapper modificando le normali `fetch` chiamate all'`fetch`API nel namespace. `AwsWafIntegration` Il AWS WAF wrapper supporta tutte le stesse opzioni della chiamata JavaScript `fetch` API standard e aggiunge la gestione dei token per l'integrazione. Questo approccio è generalmente il modo più semplice per integrare l'applicazione.

Prima dell'implementazione del wrapper

L'elenco di esempio seguente mostra il codice standard prima di implementare il `AwsWafIntegration` `fetch` wrapper.

```
const login_response = await fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
     },
     body: login_body
   });
```

Dopo l'implementazione del wrapper

L'elenco seguente mostra lo stesso codice con l'implementazione del `AwsWafIntegration` `fetch` wrapper.

```
const login_response = await AwsWafIntegration.fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
     },
     body: login_body
   });
```

Come usare l'integrazione **`getToken`**

AWS WAF richiede che le richieste agli endpoint protetti includano il cookie denominato `aws-waf-token` con il valore del token corrente.

L'`getToken`operazione è una chiamata API asincrona che recupera il AWS WAF token e lo memorizza in un cookie nella pagina corrente con il nome `aws-waf-token` e il valore impostato sul valore del token. Puoi utilizzare questo cookie token in base alle tue esigenze nella tua pagina.

Quando chiamigetToken, esegue le seguenti operazioni:

- Se un token non scaduto è già disponibile, la chiamata lo restituisce immediatamente.
- In caso contrario, la chiamata recupera un nuovo token dal fornitore del token e attende il completamento del flusso di lavoro di acquisizione del token fino a 2 secondi prima che scada il timeout. Se l'operazione scade, viene generato un errore, che deve essere gestito dal codice di chiamata.

L'getTokenoperazione è accompagnata da un'hasTokenoperazione che indica se il aws-waf-token cookie contiene attualmente un token non scaduto.

AwsWafIntegration.getToken()recupera un token valido e lo memorizza come cookie. La maggior parte delle chiamate client allega automaticamente questo cookie, ma alcune no. Ad esempio, le chiamate effettuate tra domini host non allegano il cookie. Nei dettagli di implementazione che seguono, mostriamo come lavorare con entrambi i tipi di chiamate client.

getTokenImplementazione di base, per le chiamate che allegano il **aws-waf-token** cookie

L'elenco di esempio seguente mostra il codice standard per l'implementazione dell'getTokenoperazione con una richiesta di accesso.

```
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
 }
```

Invia il modulo solo dopo che il token è disponibile da **getToken**

L'elenco seguente mostra come registrare un listener di eventi per intercettare gli invii di moduli fino a quando non sarà disponibile un token valido per l'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>
```

Allegare il token quando il client non allega il cookie per impostazione predefinita **`aws-waf-token`**

`AwsWafIntegration.getToken()`recupera un token valido e lo memorizza come cookie, ma non tutte le chiamate client associano questo cookie per impostazione predefinita. Ad esempio, le chiamate effettuate tra domini host non allegano il cookie.

Il `fetch` wrapper gestisce questi casi automaticamente, ma se non riesci a utilizzare il `fetch` wrapper, puoi gestirlo utilizzando un'intestazione personalizzata. `x-aws-waf-token` AWS WAF legge i token da questa intestazione, oltre a leggerli dal cookie. `aws-waf-token` Il codice seguente mostra un esempio di impostazione dell'intestazione.

```
const token = await AwsWafIntegration.getToken();
const result = await fetch('/url', {
    headers: {
        'x-aws-waf-token': token,
```

```
    },
});
```

Per impostazione predefinita, accetta AWS WAF solo token che contengono lo stesso dominio del dominio host richiesto. Qualsiasi token interdominio richiede le voci corrispondenti nell'elenco dei domini del token ACL Web. Per ulteriori informazioni, consulta Configurazione dell'elenco dei domini del token ACL Web.

Per ulteriori informazioni sull'uso dei token tra domini, consulta aws-samples/ -. aws-waf-bot-control api-protection-with-captcha

Utilizzo dell'API CAPTCHA JavaScript

L' JavaScript API CAPTCHA consente di configurare il puzzle CAPTCHA e posizionarlo dove si desidera nell'applicazione client. Questa API sfrutta le funzionalità delle JavaScript API intelligenti per le minacce per acquisire e utilizzare i AWS WAF token dopo che un utente finale ha completato con successo un puzzle CAPTCHA.

Implementa l' JavaScript integrazione prima in un ambiente di test, poi in produzione. Per ulteriori indicazioni sulla codifica, consulta le sezioni seguenti.

Per utilizzare l'API di integrazione CAPTCHA

1. Installa l'API

    a. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
    b. Nel riquadro di navigazione, scegliere Application integration (Integrazione di applicazioni). Nella pagina di integrazione dell'applicazione, puoi vedere le opzioni a schede.
    c. Seleziona Integrazione CAPTCHA.
    d. Copia il tag dello script di JavaScript integrazione elencato per utilizzarlo nella tua integrazione.
    e. Nel codice della pagina dell'applicazione, nella <head> sezione, inserisci il tag script che hai copiato. Questa inclusione rende il puzzle CAPTCHA disponibile per la configurazione e l'uso.

    ```
    <head>
        <script type="text/javascript" src="integrationURL/jsapi.js" defer></
    script>
    ```

```
</head>
```

Questo `<script>` elenco è configurato con l'`defer`attributo, ma puoi modificare l'impostazione `async` se desideri un comportamento diverso per la tua pagina.

Lo script CAPTCHA carica automaticamente anche lo script di integrazione intelligente delle minacce se non è già presente. Lo script di integrazione intelligente delle minacce consente all'applicazione client di recuperare automaticamente un token in background al caricamento della pagina e fornisce altre funzionalità di gestione dei token necessarie per l'utilizzo dell'API CAPTCHA.

2. (Facoltativo) Aggiungi la configurazione del dominio per i token del client: per impostazione predefinita, quando AWS WAF crea un token, utilizza il dominio host della risorsa associata all'ACL web. Per fornire domini aggiuntivi per le JavaScript API, segui le indicazioni all'indirizzo. Fornire domini da utilizzare nei token
3. Ottieni la chiave API crittografata per il client: l'API CAPTCHA richiede una chiave API crittografata che contenga un elenco di domini client validi. AWS WAF utilizza questa chiave per verificare che il dominio client che stai utilizzando con l'integrazione sia approvato per l'uso di CAPTCHA. AWS WAF Per generare la tua chiave API, segui le istruzioni all'indirizzo. Gestione delle chiavi API per l'API JS CAPTCHA
4. Codifica l'implementazione del widget CAPTCHA: implementa la chiamata `renderCaptcha()` API nella tua pagina, nel luogo in cui desideri utilizzarla. Per informazioni sulla configurazione e l'uso di questa funzione, consulta le seguenti sezioni e. Specifiche dell'API CAPTCHA JavaScript Come renderizzare il puzzle CAPTCHA

   L'implementazione CAPTCHA si integra con le API di integrazione intelligente delle minacce per la gestione dei token e per l'esecuzione di chiamate di recupero che utilizzano i token. AWS WAF Per indicazioni sull'utilizzo di queste API, consulta. Utilizzo dell' JavaScript API per le minacce intelligenti
5. Aggiungi la verifica tramite token nell'ACL Web: aggiungi almeno una regola all'ACL Web per verificare la presenza di un token CAPTCHA valido nelle richieste Web inviate dal client. Puoi utilizzare l'azione della CAPTCHA regola per verificare, come descritto in. CAPTCHAe Challenge in AWS WAF

   Le aggiunte Web ACL verificano che le richieste dirette agli endpoint protetti includano il token che hai acquisito nell'integrazione con il client. Le richieste che includono un token CAPTCHA valido e non scaduto superano l'ispezione delle CAPTCHA regole e non presentano all'utente finale un altro puzzle CAPTCHA.

Argomenti

Specifiche dell'API CAPTCHA JavaScript

Questa sezione elenca le specifiche per i metodi e le proprietà delle API CAPTCHA JavaScript . Usa le JavaScript API CAPTCHA per eseguire puzzle CAPTCHA personalizzati nelle tue applicazioni client.

Questa API si basa sulle API intelligenti per le minacce, che utilizzi per configurare e gestire l'acquisizione e l'utilizzo dei token. AWS WAF VediSpecifiche dell'API per le minacce intelligenti.

`AwsWafCaptcha.renderCaptcha(container, configuration)`

Presenta un puzzle AWS WAF CAPTCHA all'utente finale e, in caso di successo, aggiorna il token client con la convalida CAPTCHA. Questo è disponibile solo con l'integrazione CAPTCHA. Utilizza questa chiamata insieme alle API intelligenti per le minacce per gestire il recupero dei token e fornire il token nelle chiamate. `fetch` Consulta le API per le minacce intelligenti all'indirizzo. Specifiche dell'API per le minacce intelligenti

A differenza del CAPTCHA interstitial che AWS WAF invia, il puzzle CAPTCHA reso con questo metodo visualizza il puzzle immediatamente, senza una schermata iniziale del titolo.

`container`

L'`Element`oggetto per l'elemento contenitore di destinazione sulla pagina. Questo viene in genere recuperato chiamando `document.getElementById()` o`document.querySelector()`.

Campo obbligatorio: sì

Tipo: `Element`

configurazione

Un oggetto contenente le impostazioni di configurazione CAPTCHA, come segue:

`apiKey`

La chiave API crittografata che abilita le autorizzazioni per il dominio del client. Usa la AWS WAF console per generare le tue chiavi API per i domini dei tuoi clienti. Puoi utilizzare una chiave per un massimo di cinque domini. Per informazioni, consulta Gestione delle chiavi API per l'API JS CAPTCHA.

Campo obbligatorio: sì

Tipo: `string`

`onSuccess: (wafToken: string) => void;`

Chiamato con un AWS WAF token valido quando l'utente finale completa con successo un puzzle CAPTCHA. Usa il token nelle richieste che invii agli endpoint che proteggi con un ACL web. AWS WAF Il token fornisce la prova e il timestamp dell'ultimo completamento riuscito del puzzle.

Campo obbligatorio: sì

`onError?: (error: CaptchaError) => void;`

Chiamato con un oggetto error quando si verifica un errore durante l'operazione CAPTCHA.

Campo obbligatorio: no

`CaptchaError`definizione della classe — Il `onError` gestore fornisce un tipo di errore con la seguente definizione di classe.

```
CaptchaError extends Error {
    kind: "internal_error" | "network_error" | "token_error" | "client_error";
    statusCode?: number;
}
```

- `kind`— Il tipo di errore restituito.
- `statusCode`— Il codice di stato HTTP, se disponibile. Viene utilizzato da `network_error` se l'errore è dovuto a un errore HTTP.

`onLoad?: () => void;`

Chiamato quando viene caricato un nuovo puzzle CAPTCHA.

Campo obbligatorio: no

`onPuzzleTimeout?: () => void;`

Chiamato quando un puzzle CAPTCHA non viene completato prima della scadenza.

Campo obbligatorio: no

`onPuzzleCorrect?: () => void;`

Chiamato quando viene fornita una risposta corretta a un puzzle CAPTCHA.

Campo obbligatorio: no

`onPuzzleIncorrect?: () => void;`

Chiamato quando viene fornita una risposta errata a un puzzle CAPTCHA.

Campo obbligatorio: no

`defaultLocale`

La localizzazione predefinita da usare per il puzzle CAPTCHA. Le istruzioni scritte per i puzzle CAPTCHA sono disponibili in arabo (ar-SA), cinese semplificato (zh-CN), olandese (nl-NL), inglese (en-US), francese (fr-FR), tedesco (de-DE), italiano (it-IT), giapponese (ja-JP), portoghese brasiliano (pt-BR), spagnolo (es-ES) e turco (tr-TR). Le istruzioni audio sono disponibili per tutte le lingue scritte tranne il cinese e il giapponese, che per impostazione predefinita è l'inglese. Per cambiare la lingua predefinita, fornisci la lingua internazionale e il codice locale, ad esempio`ar-SA`.

Predefinita: la lingua attualmente in uso nel browser dell'utente finale

Campo obbligatorio: no

Tipo: `string`

`disableLanguageSelector`

Se impostato su`true`, il puzzle CAPTCHA nasconde il selettore della lingua.

Impostazione predefinita: `false`

Campo obbligatorio: no

Tipo: `boolean`

`dynamicWidth`

Se impostato su`true`, il puzzle CAPTCHA cambia larghezza per compatibilità con la larghezza della finestra del browser.

Impostazione predefinita: `false`

Campo obbligatorio: no

Tipo: `boolean`

`skipTitle`

Se impostato su**`true`**, il puzzle CAPTCHA non visualizza il titolo del puzzle Risolvi il puzzle.

Impostazione predefinita: `false`

Campo obbligatorio: no

Tipo: `boolean`

Come renderizzare il puzzle CAPTCHA

È possibile utilizzare la AWS WAF `renderCaptcha` chiamata dove si desidera nell'interfaccia client. La chiamata recupera un puzzle CAPTCHA da AWS WAF, lo esegue il rendering e invia i risultati per la verifica. AWS WAF Quando effettui la chiamata, fornisci la configurazione di rendering del puzzle e i callback che desideri eseguire quando gli utenti finali completano il puzzle. Per informazioni dettagliate sulle opzioni, consultate la sezione precedente,. Specifiche dell'API CAPTCHA JavaScript

Utilizzate questa chiamata insieme alla funzionalità di gestione dei token delle API di integrazione intelligente delle minacce. Questa chiamata fornisce al cliente un token che verifica il completamento con successo del puzzle CAPTCHA. Utilizzate le API di integrazione intelligente delle minacce per gestire il token e fornire il token nelle chiamate del cliente agli endpoint protetti con ACL Web. AWS WAF Per informazioni sulle API per le minacce intelligenti, consulta. Utilizzo dell' JavaScript API per le minacce intelligenti

Esempio di implementazione

L'elenco di esempio seguente mostra un'implementazione CAPTCHA standard, incluso il posizionamento dell'URL di AWS WAF integrazione nella <head> sezione.

Questo elenco configura la `renderCaptcha` funzione con un callback di successo che utilizza il `AwsWafIntegration.fetch` wrapper delle API di integrazione intelligente delle minacce. Per informazioni su questa funzione, vedere. Come usare il `fetch` wrapper di integrazione

```
<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>
```

Impostazioni di configurazione di esempio

L'elenco di esempio seguente mostra le opzioni `renderCaptcha` con impostazioni non predefinite per la larghezza e il titolo.

```
        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            dynamicWidth: true,
            skipTitle: true
        });
```

Per informazioni complete sulle opzioni di configurazione, vedereSpecifiche dell'API CAPTCHA JavaScript .

Gestione di una risposta CAPTCHA da AWS WAF

Una AWS WAF regola con un'CAPTCHAazione interrompe la valutazione di una richiesta web corrispondente se la richiesta non ha un token con un timestamp CAPTCHA valido. Se la richiesta è una chiamata `GET` text/html, l'CAPTCHAazione invia al client un messaggio interstiziale con un puzzle CAPTCHA. Quando non integri l' JavaScript API CAPTCHA, l'interstitial esegue il puzzle e, se l'utente finale lo risolve con successo, invia nuovamente la richiesta automaticamente.

Quando integri l' JavaScript API CAPTCHA e personalizzi la gestione del CAPTCHA, devi rilevare la risposta CAPTCHA di terminazione, fornire il CAPTCHA personalizzato e, se l'utente finale risolve con successo il puzzle, inviare nuovamente la richiesta web del cliente.

L'esempio di codice seguente mostra come eseguire tale operazione.

> **Note**
>
> La risposta AWS WAF CAPTCHA all'azione ha un codice di stato HTTP 405, che utilizziamo per riconoscere la risposta in questo codice. CAPTCHA Se l'endpoint protetto utilizza un codice di stato HTTP 405 per comunicare qualsiasi altro tipo di risposta per la stessa chiamata, questo codice di esempio genererà anche un puzzle CAPTCHA per quelle risposte.

```
<!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>
```

Gestione delle chiavi API per l'API JS CAPTCHA

Per integrare AWS WAF CAPTCHA in un'applicazione client con l' JavaScript API, sono necessari il tag di integrazione JavaScript API e la chiave API crittografata per il dominio client in cui desideri eseguire il puzzle CAPTCHA.

L'integrazione dell'applicazione CAPTCHA JavaScript utilizza le chiavi API crittografate per verificare che il dominio dell'applicazione client sia autorizzato a utilizzare l'API CAPTCHA. AWS WAF Quando richiami l'API CAPTCHA dal tuo JavaScript client, fornisci una chiave API con un elenco di domini che include un dominio per il client corrente. Puoi elencare fino a 5 domini in un'unica chiave crittografata.

Requisiti delle chiavi API

La chiave API che utilizzi nell'integrazione CAPTCHA deve contenere un dominio applicabile al client in cui utilizzi la chiave.

- Se specifichi una `window.awsWafCookieDomainList` nell'integrazione intelligente delle minacce del tuo client, almeno un dominio nella tua chiave API deve corrispondere esattamente a uno dei domini token in `window.awsWafCookieDomainList` o deve essere il dominio apex di uno di quei domini token.

  Ad esempio, per il dominio token`mySubdomain.myApex.com`, la chiave `mySubdomain.myApex.com` API corrisponde esattamente e la chiave API `myApex.com` è il dominio apex. Entrambe le chiavi corrispondono al dominio del token.

  Per informazioni sull'impostazione dell'elenco dei domini dei token, vedereFornire domini da utilizzare nei token.
- Altrimenti, il dominio corrente deve essere contenuto nella chiave API. Il dominio corrente è il dominio che puoi vedere nella barra degli indirizzi del browser.

I domini che utilizzi devono essere accettati, in base al dominio host protetto e all'elenco di domini token configurato per l'ACL web. AWS WAF Per ulteriori informazioni, consulta Configurazione dell'elenco dei domini del token ACL Web.

Come scegliere la regione per la tua chiave API

AWS WAF può generare chiavi API CAPTCHA in qualsiasi regione in cui AWS WAF sia disponibile.

Come regola generale, dovresti usare la stessa regione per la tua chiave API CAPTCHA che usi per il tuo ACL web. Se ti aspetti un pubblico globale per un ACL web regionale, tuttavia, puoi ottenere un tag di JavaScript integrazione CAPTCHA con ambito e una chiave API con ambito CloudFront e utilizzarli CloudFront con un ACL web regionale. Questo approccio consente ai clienti di caricare un puzzle CAPTCHA dalla regione a loro più vicina, il che riduce la latenza.

Le chiavi API CAPTCHA destinate a regioni diverse da quelle non CloudFront sono supportate per l'uso in più regioni. Possono essere utilizzate solo nella regione a cui sono destinate.

Per generare una chiave API per i domini dei tuoi clienti

Per ottenere l'URL di integrazione e generare e recuperare le chiavi API tramite la console.

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, scegliere Application integration (Integrazione di applicazioni).
3. Nel riquadro, ACL Web abilitati per l'integrazione delle applicazioni, seleziona la regione che desideri utilizzare per la tua chiave API. Puoi anche selezionare la regione nel riquadro delle chiavi API della scheda di integrazione CAPTCHA.
4. Scegli la scheda Integrazione CAPTCHA. Questa scheda fornisce il tag di JavaScript integrazione CAPTCHA, che puoi utilizzare nella tua integrazione, e l'elenco delle chiavi API. Entrambi si riferiscono alla regione selezionata.
5. Nel riquadro Chiavi API, scegli Genera chiave. Viene visualizzata la finestra di dialogo per la generazione delle chiavi.
6. Inserisci i domini client che desideri includere nella chiave. Puoi inserire fino a 5. Quando hai finito, scegli Genera chiave. L'interfaccia torna alla scheda di integrazione CAPTCHA, dove è elencata la tua nuova chiave.

   Una volta creata, una chiave API è immutabile. Se devi apportare modifiche a una chiave, genera una nuova chiave e usala al suo posto.
7. (Facoltativo) Copia la chiave appena generata per utilizzarla nella tua integrazione.

Per questo lavoro puoi anche utilizzare le API REST o uno degli AWS SDK specifici della lingua. Le chiamate API REST sono CreateApiKey e ListApiKeys.

Per eliminare una chiave API

Per eliminare una chiave API, devi utilizzare l'API REST o uno degli AWS SDK specifici della lingua. La chiamata all'API REST è DeleteApiKey. Non puoi utilizzare la console per eliminare una chiave.

Dopo aver eliminato una chiave, possono essere necessarie fino a 24 ore prima che non AWS WAF venga consentita l'utilizzo della chiave in tutte le aree geografiche.

AWS WAF integrazione di applicazioni mobili

Puoi utilizzare gli SDK AWS WAF mobili per implementare SDK di integrazione AWS WAF intelligente delle minacce per applicazioni mobili Android e iOS.

- Per le app mobili Android, gli AWS WAF SDK funzionano per l'API Android versione 23 (Android versione 6) e successive. Per informazioni sulle versioni di Android, consulta le note di rilascio della piattaforma SDK.
- Per le app mobili iOS, AWS WAF gli SDK funzionano per iOS versione 13 e successive. Per informazioni sulle versioni di iOS, consulta le note di rilascio di iOS e iPadOS.

Con l'SDK per dispositivi mobili, puoi gestire l'autorizzazione dei token e includerli nelle richieste inviate alle tue risorse protette. Utilizzando gli SDK, ti assicuri che queste chiamate di procedura remota da parte del tuo client contengano un token valido. Inoltre, quando questa integrazione è attiva nelle pagine dell'applicazione, puoi implementare regole di mitigazione nell'ACL web, come bloccare le richieste che non contengono un token valido.

Per accedere agli SDK per dispositivi mobili, contatta l'assistenza all'indirizzo Contact. AWS

> **Note**
>
> Gli SDK AWS WAF per dispositivi mobili non sono disponibili per la personalizzazione dei CAPTCHA.

L'approccio di base per l'utilizzo dell'SDK consiste nel creare un provider di token utilizzando un oggetto di configurazione, quindi utilizzare il provider di token da cui recuperare i token. AWS WAF Per impostazione predefinita, il provider di token include i token recuperati nelle richieste web alla risorsa protetta.

Di seguito è riportato un elenco parziale di un'implementazione SDK, che mostra i componenti principali. Per esempi più dettagliati, consulta Scrivere il codice per l'SDK AWS WAF mobile.

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();
```

Installazione dell'SDK AWS WAF per dispositivi mobili

Per accedere agli SDK per dispositivi mobili, contatta l'assistenza all'indirizzo Contact AWS.

Implementa l'SDK mobile prima in un ambiente di test, poi in produzione.

Per installare l'SDK AWS WAF mobile

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, scegliere Application integration (Integrazione di applicazioni).
3. Nella scheda Integrazioni intelligenti contro le minacce, procedi come segue:

   a. Nel riquadro ACL Web abilitati per l'integrazione delle applicazioni, individua l'ACL Web con cui stai effettuando l'integrazione. Copia e salva l'URL di integrazione ACL Web da utilizzare nell'implementazione. Puoi ottenere questo URL anche tramite la chiamata `GetWebACL` API.

   b. Scegli il tipo e la versione del dispositivo mobile, quindi scegli Scarica. Puoi scegliere la versione che preferisci, ma ti consigliamo di utilizzare la versione più recente. AWS WAF scarica il `zip` file per il tuo dispositivo nella posizione di download standard.

4. Nell'ambiente di sviluppo dell'app, decomprimi il file in una posizione di lavoro a tua scelta. Nella directory di primo livello del file zip, individua e apri il `README` Segui le istruzioni contenute nel `README` file per installare l'SDK per AWS WAF dispositivi mobili da utilizzare nel codice dell'app per dispositivi mobili.
5. Programma la tua app in base alle indicazioni riportate nelle sezioni seguenti.

Le specifiche SDK AWS WAF per dispositivi mobili

Questa sezione elenca gli oggetti SDK, le operazioni e le impostazioni di configurazione per l'ultima versione disponibile dell'SDK AWS WAF mobile. Per informazioni dettagliate su come funzionano il provider di token e le operazioni per le varie combinazioni di impostazioni di configurazione, consulta. Come funziona l'SDK AWS WAF per dispositivi mobili

`WAFToken`

Detiene un AWS WAF token.

`getValue()`

Recupera la `String` rappresentazione di. `WAFToken`

`WAFTokenProvider`

Gestisce i token nella tua app mobile. Implementalo usando un `WAFConfiguration` oggetto.

`getToken()`

Se l'aggiornamento in background è abilitato, restituisce il token memorizzato nella cache. Se l'aggiornamento in background è disabilitato, viene effettuata una chiamata sincrona e bloccante AWS WAF a per recuperare un nuovo token.

`onTokenReady(WAFTokenResultCallback)`

Indica al fornitore del token di aggiornare il token e di richiamare il callback fornito quando un token attivo è pronto. Il fornitore del token invocherà il callback in un thread in background quando il token è memorizzato nella cache e pronto. Chiamalo quando l'app viene caricata per la prima volta e anche quando torna allo stato attivo. Per ulteriori informazioni sul ritorno a uno stato attivo, consultathe section called “Recupero di un token dopo l'inattività dell'app”.

Per le app Android o iOS, puoi `WAFTokenResultCallback` impostare l'operazione che desideri venga richiamata dal provider del token quando un token richiesto è pronto. La tua implementazione di `WAFTokenResultCallback` deve accettare i

parametriWAFToken,SdkError. Per le app iOS, puoi creare alternativamente una funzione in linea.

storeTokenInCookieStorage(WAFToken)

Indica WAFTokenProvider a memorizzare il AWS WAF token specificato nel gestore dei cookie dell'SDK. Per impostazione predefinita, il token viene aggiunto all'archivio dei cookie solo quando viene acquisito per la prima volta e quando viene aggiornato. Se l'applicazione cancella l'archivio di cookie condiviso per qualsiasi motivo, l'SDK non aggiunge automaticamente il AWS WAF token fino al prossimo aggiornamento.

WAFConfiguration

Contiene la configurazione per l'implementazione di. WAFTokenProvider Quando lo implementate, fornite l'URL di integrazione dell'ACL Web, il nome di dominio da utilizzare nel token e tutte le impostazioni non predefinite che desiderate che il provider del token utilizzi.

L'elenco seguente specifica le impostazioni di configurazione che è possibile gestire nell'oggetto. WAFConfiguration

applicationIntegrationUrl

L'URL di integrazione dell'applicazione. Scaricalo dalla AWS WAF console o tramite la chiamata getWebACL API.

Campo obbligatorio: sì

Tipo: URL specifico dell'app. Per iOS, vedi URL iOS. Per Android, vedi l'URL java.net.

backgroundRefreshEnabled

Indica se desideri che il fornitore del token aggiorni il token in background. Se si imposta questa impostazione, il provider di token aggiorna i token in background in base alle impostazioni di configurazione che regolano le attività di aggiornamento automatico dei token.

Campo obbligatorio: no

Tipo: Boolean

Valore predefinito: TRUE

domainName

Il dominio da utilizzare nel token, utilizzato per l'acquisizione dei token e l'archiviazione dei cookie. Ad esempio example.com o aws.amazon.com. Di solito si tratta del dominio host

della risorsa associato all'ACL web, a cui invierai le richieste web. Per il gruppo di regole gestito ACFP`AWSManagedRulesACFPRuleSet`, in genere si tratta di un singolo dominio che corrisponde al dominio nel percorso di creazione dell'account fornito nella configurazione del gruppo di regole. Per il gruppo di regole gestito ATP`AWSManagedRulesATPRuleSet`, in genere si tratta di un singolo dominio che corrisponde al dominio nel percorso di accesso fornito nella configurazione del gruppo di regole.

I suffissi pubblici non sono consentiti. Ad esempio, non puoi usare `gov.au` or `co.uk` come dominio del token.

Il dominio deve essere accettato, in base al dominio host protetto e all'elenco di domini token dell'ACL Web. AWS WAF Per ulteriori informazioni, consulta Configurazione dell'elenco dei domini del token ACL Web.

Campo obbligatorio: sì

Tipo: `String`

`maxErrorTokenRefreshDelayMsec`

Il tempo massimo di attesa in millisecondi prima di ripetere un aggiornamento del token dopo un tentativo fallito. Questo valore viene utilizzato dopo che il recupero del token non è riuscito ed è stato ripetuto più volte. `maxRetryCount`

Campo obbligatorio: no

Tipo: `Integer`

Valore predefinito: `5000` (5 secondi)

Valore minimo consentito: 1 (1 millisecondo)

Valore massimo consentito: `30000` (30 secondi)

`maxRetryCount`

Il numero massimo di tentativi da eseguire con backoff esponenziale quando viene richiesto un token.

Campo obbligatorio: no

Tipo: `Integer`

Valore predefinito: se l'aggiornamento in background è abilitato,. `5` In caso contrario, `3`.

Valore minimo consentito: `0`

Valore massimo consentito: `10`

`setTokenCookie`

Indica se desideri che il gestore dei cookie dell'SDK aggiunga un cookie token nelle tue richieste. Per impostazione predefinita, questo aggiunge un cookie token a tutte le richieste. Il gestore dei cookie aggiunge un cookie token a qualsiasi richiesta il cui percorso si trova nel percorso specificato in`tokenCookiePath`.

Campo obbligatorio: no

Tipo: `Boolean`

Valore predefinito: `TRUE`

`tokenCookiePath`

Usato quando `setTokenCookie` è`TRUE`. Indica il percorso di primo livello in cui desideri che il gestore dei cookie dell'SDK aggiunga un cookie token. Il gestore aggiunge un cookie token a tutte le richieste inviate a questo percorso e a tutti i percorsi secondari.

Ad esempio, se lo imposti su`/web/login`, il gestore include il cookie token per tutto ciò che viene inviato `/web/login` e per tutti i relativi percorsi secondari, ad esempio`/web/login/help`. Non include il token per le richieste inviate ad altri percorsi, come `//web`, o`/web/order`.

Campo obbligatorio: no

Tipo: `String`

Valore predefinito: `/`

`tokenRefreshDelaySec`

Utilizzato per l'aggiornamento dello sfondo. La quantità massima di tempo in secondi tra gli aggiornamenti dei token in background.

Campo obbligatorio: no

Tipo: `Integer`

Valore predefinito: 88

Valore minimo consentito: 88

Valore massimo consentito: `300` (5 minuti)

Come funziona l'SDK AWS WAF per dispositivi mobili

Gli SDK per dispositivi mobili forniscono un provider di token configurabile che è possibile utilizzare per il recupero e l'utilizzo dei token. Il fornitore di token verifica che le richieste consentite provengano da clienti legittimi. Quando invii richieste alle AWS risorse con cui proteggi AWS WAF, includi il token in un cookie per convalidare la richiesta. Puoi gestire il cookie del token manualmente o lasciare che sia il fornitore del token a farlo per te.

Questa sezione tratta le interazioni tra le classi, le proprietà e i metodi inclusi nell'SDK per dispositivi mobili. Per le specifiche dell'SDK, consulta. Le specifiche SDK AWS WAF per dispositivi mobili

Recupero e memorizzazione nella cache dei token

Quando crei l'istanza del fornitore di token nella tua app per dispositivi mobili, configuri come desideri che gestisca i token e il recupero dei token. La tua scelta principale è come mantenere i token validi e non scaduti da utilizzare nelle richieste web dell'app:

- Aggiornamento in background abilitato: questa è l'impostazione predefinita. Il provider del token aggiorna automaticamente il token in background e lo memorizza nella cache. Con l'aggiornamento in background abilitato, quando si chiama`getToken()`, l'operazione recupera il token memorizzato nella cache.

  Il provider del token esegue l'aggiornamento del token a intervalli configurabili, in modo che un token non scaduto sia sempre disponibile nella cache mentre l'applicazione è attiva. L'aggiornamento in background viene sospeso mentre l'applicazione è in uno stato inattivo. Per informazioni su questo argomento, vedere. Recupero di un token dopo l'inattività dell'app
- Aggiornamento in background disabilitato: è possibile disabilitare l'aggiornamento dei token in background e quindi recuperare i token solo su richiesta. I token recuperati su richiesta non vengono memorizzati nella cache e, se lo desideri, puoi recuperarne più di uno. Ogni token è indipendente dagli altri che recuperi e ognuno ha il proprio timestamp che viene utilizzato per calcolare la scadenza.

  Hai le seguenti scelte per il recupero dei token quando l'aggiornamento in background è disabilitato:

- **`getToken()`**— Quando si chiama `getToken()` con l'aggiornamento in background disabilitato, la chiamata recupera in modo sincrono un nuovo token da. AWS WAF Si tratta di una chiamata potenzialmente bloccante che può influire sulla reattività dell'app se viene richiamata nel thread principale.
- **`onTokenReady(WAFTokenResultCallback)`**— Questa chiamata recupera in modo asincrono un nuovo token e quindi richiama il callback dei risultati fornito in un thread in background quando un token è pronto.

In che modo il fornitore del token tenta di ripetere i recuperi di token non riusciti

Il fornitore di token riprova automaticamente il recupero del token quando il recupero fallisce. I nuovi tentativi vengono inizialmente eseguiti utilizzando il backoff esponenziale con un tempo di attesa iniziale di 100 ms. Per informazioni sui tentativi esponenziali, vedere Tentativi di errore e backoff esponenziale in. AWS

Quando il numero di tentativi raggiunge il valore configuratomaxRetryCount, il fornitore del token smette di provare o passa a provare ogni `maxErrorTokenRefreshDelayMsec` millisecondo, a seconda del tipo di recupero del token:

- **`onTokenReady()`**— Il fornitore del token passa ad attendere `maxErrorTokenRefreshDelayMsec` millisecondi tra un tentativo e l'altro e continua a cercare di recuperare il token.
- Aggiornamento in background: il fornitore del token passa ad attendere `maxErrorTokenRefreshDelayMsec` millisecondi tra un tentativo e l'altro e continua a cercare di recuperare il token.
- **`getToken()`**Chiamate su richiesta, quando l'aggiornamento in background è disabilitato: il provider di token interrompe il tentativo di recuperare un token e restituisce il valore del token precedente o un valore nullo se non esiste un token precedente.

Recupero di un token dopo l'inattività dell'app

L'aggiornamento in background viene eseguito solo quando l'app è considerata attiva per il tipo di app in uso:

- iOS: l'aggiornamento in background viene eseguito quando l'app è in primo piano.
- Android: l'aggiornamento in background viene eseguito quando l'app non è chiusa, indipendentemente dal fatto che sia in primo piano o in background.

Se l'app rimane in uno stato che non supporta l'aggiornamento in background per un periodo superiore ai `tokenRefreshDelaySec` secondi configurati, il fornitore del token sospende l'aggiornamento in background. Ad esempio, per un'app iOS, se `tokenRefreshDelaySec` è 300 e l'app si chiude o passa in background per più di 300 secondi, il fornitore del token interrompe l'aggiornamento del token. Quando l'app torna a uno stato attivo, il provider del token riavvia automaticamente l'aggiornamento in background.

Quando l'app torna allo stato attivo, chiama `onTokenReady()` per ricevere una notifica quando il fornitore del token ha recuperato e memorizzato nella cache un nuovo token. Non limitarti a chiamare`getToken()`, perché la cache potrebbe non contenere ancora un token attuale e valido.

Scrivere il codice per l'SDK AWS WAF mobile

Questa sezione fornisce esempi di codice per l'utilizzo dell'SDK per dispositivi mobili.

Inizializzazione del fornitore di token e ottenimento dei token

Si avvia l'istanza del provider di token utilizzando un oggetto di configurazione. Quindi puoi recuperare i token utilizzando le operazioni disponibili. Di seguito vengono illustrati i componenti di base del codice richiesto.

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

```
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();
```

Consentire all'SDK di fornire il cookie del token nelle richieste HTTP

In caso `setTokenCookie` affermativo`TRUE`, il fornitore del token include il cookie del token nelle richieste web a tutte le località nel percorso specificato in`tokenCookiePath`. Per impostazione predefinita, `setTokenCookie` è `TRUE` ed `tokenCookiePath` è`/`.

È possibile restringere l'ambito delle richieste che includono un cookie token specificando il percorso del cookie del token, `/web/login` ad esempio. Se lo fai, controlla che AWS WAF le tue regole non controllino la presenza di token nelle richieste che invii ad altri percorsi. Quando utilizzi il

gruppo di `AWSManagedRulesACFPRuleSet` regole, configuri i percorsi di registrazione e creazione dell'account e il gruppo di regole verifica la presenza di token nelle richieste inviate a tali percorsi. Per ulteriori informazioni, consulta Aggiungere il gruppo di regole gestite ACFP all'ACL Web. Allo stesso modo, quando si utilizza il gruppo di `AWSManagedRulesATPRuleSet` regole, si configura il percorso di accesso e il gruppo di regole verifica la presenza di token nelle richieste inviate a quel percorso. Per ulteriori informazioni, consulta Aggiungere il gruppo di regole gestite da ATP all'ACL Web.

iOS

In caso `setTokenCookie` TRUE affermativo, il fornitore del AWS WAF token memorizza il token in un file `HTTPCookieStorage.shared` e lo include automaticamente nelle richieste al dominio specificato in`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

In caso `setTokenCookie` TRUE affermativo, il provider del token archivia il AWS WAF token in un'`CookieHandler`istanza condivisa a livello di applicazione. Il provider di token include automaticamente il cookie nelle richieste al dominio specificato dall'utente`WAFConfiguration`.

```
URL url = new URL("Domain name");
 //The token cookie is set automatically as cookie header
 HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
 connection.getResponseCode();
```

Se hai già inizializzato l'istanza `CookieHandler` predefinita, il fornitore del token la utilizzerà per gestire i cookie. In caso contrario, il fornitore del token inizializzerà una nuova `CookieManager` istanza con il AWS WAF token `CookiePolicy.ACCEPT_ORIGINAL_SERVER` e quindi imposterà questa nuova istanza come istanza predefinita in. `CookieHandler`

Il codice seguente mostra come l'SDK inizializza il gestore dei cookie e il gestore dei cookie quando non sono disponibili nell'app.

```
CookieManager cookieManager = (CookieManager) CookieHandler.getDefault();
 if (cookieManager == null) {
     // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
     cookieManager = new CookieManager();
```

```
    CookieHandler.setDefault(cookieManager);
}
```

Fornire manualmente il cookie del token nelle richieste HTTP

Se lo `setTokenCookie` impostiFALSE, devi fornire il cookie token manualmente, come intestazione della richiesta Cookie HTTP, nelle tue richieste all'endpoint protetto. Il codice seguente mostra come eseguire questa operazione.

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

```
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();
```

CAPTCHAe Challenge in AWS WAF

Puoi configurare AWS WAF le tue regole per eseguire un'Challengeazione CAPTCHA o un'azione contro le richieste web che soddisfano i criteri di ispezione della regola. Puoi anche programmare le tue applicazioni JavaScript client per eseguire i puzzle CAPTCHA e le sfide del browser a livello locale.

- CAPTCHA— Richiede all'utente finale di risolvere un puzzle CAPTCHA per dimostrare che un essere umano sta inviando la richiesta. I puzzle CAPTCHA sono pensati per essere abbastanza facili e veloci da completare con successo per gli esseri umani e difficili da completare per i computer, con successo o in modo casuale con un tasso di successo significativo.

  Nelle regole ACL web, CAPTCHA viene comunemente utilizzato quando un'Blockazione bloccherebbe troppe richieste legittime, ma lasciare passare tutto il traffico comporterebbe livelli

inaccettabilmente elevati di richieste indesiderate, ad esempio provenienti da bot. Per informazioni sul comportamento delle regole, consulta. Come funzionano le azioni CAPTCHA e le Challenge regole

Puoi anche programmare un'implementazione di puzzle CAPTCHA nelle API di integrazione delle applicazioni client. Quando lo fai, puoi personalizzare il comportamento e il posizionamento del puzzle nell'applicazione client. Per ulteriori informazioni, consulta AWS WAF integrazione delle applicazioni client.

- Challenge— Esegue una sfida silenziosa che richiede che la sessione client verifichi che si tratti di un browser e non di un bot. La verifica viene eseguita in background senza coinvolgere l'utente finale. Questa è una buona opzione per verificare i client che sospetti non siano validi senza influire negativamente sull'esperienza dell'utente finale con un puzzle CAPTCHA. Per informazioni sul comportamento delle regole, consulta. Come funzionano le azioni CAPTCHA e le Challenge regole

  L'azione della Challenge regola è simile alla sfida gestita dalle API Client Intelligent Threat Integration, descritta inAWS WAF integrazione delle applicazioni client.

> **Note**
>
> Ti vengono addebitati costi aggiuntivi quando utilizzi l'azione CAPTCHA o Challenge regola in una delle tue regole o come regola che sostituisce un'azione in un gruppo di regole. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

Per una descrizione di tutte le opzioni di azione delle regole, consultaOperazione delle regole.

Argomenti

- AWS WAF Puzzle CAPTCHA
- Come funzionano le azioni CAPTCHA e le Challenge regole
- Procedure consigliate per l'utilizzo Challenge delle azioni CAPTCHA e

AWS WAF Puzzle CAPTCHA

AWS WAF fornisce una funzionalità CAPTCHA standard che sfida gli utenti a confermare che si tratta di esseri umani. CAPTCHA è l'acronimo di Completely Automated Public Turing test per distinguere computer e umani. I puzzle CAPTCHA sono progettati per verificare che un essere

umano stia inviando richieste e per prevenire attività come il web scraping, il furto di credenziali e lo spam. I puzzle CAPTCHA non possono eliminare tutte le richieste indesiderate. Molti enigmi sono stati risolti utilizzando l'apprendimento automatico e l'intelligenza artificiale. Nel tentativo di aggirare il CAPTCHA, alcune organizzazioni integrano tecniche automatizzate con l'intervento umano. Nonostante ciò, CAPTCHA continua a essere uno strumento utile per prevenire il traffico di bot meno sofisticato e per aumentare le risorse necessarie per operazioni su larga scala.

AWS WAF genera casualmente i propri puzzle CAPTCHA e li percorre a rotazione per garantire che gli utenti si trovino di fronte a sfide uniche. AWS WAF aggiunge regolarmente nuovi tipi e stili di puzzle per rimanere efficace contro le tecniche di automazione. Oltre ai puzzle, lo script AWS WAF CAPTCHA raccoglie dati sul client per garantire che l'attività venga completata da un essere umano e per prevenire attacchi di replay.

Ogni puzzle CAPTCHA include un set standard di controlli che consentono all'utente finale di richiedere un nuovo puzzle, passare da un puzzle audio a uno visivo e viceversa, accedere a istruzioni aggiuntive e inviare una soluzione al puzzle. Tutti i puzzle includono il supporto per screen reader, controlli da tastiera e colori contrastanti.

I puzzle AWS WAF CAPTCHA soddisfano i requisiti delle Web Content Accessibility Guidelines (WCAG). Per informazioni, consulta la panoramica delle linee guida per l'accessibilità dei contenuti Web (WCAG) sul sito Web del World Wide Web Consortium (W3C).

Argomenti

- Supporto per il linguaggio dei puzzle CAPTCHA
- Esempi di puzzle CAPTCHA

Supporto per il linguaggio dei puzzle CAPTCHA

Il puzzle CAPTCHA inizia con istruzioni scritte nella lingua del browser del client o, se la lingua del browser non è supportata, in inglese. Il puzzle offre opzioni di lingua alternative tramite un menu a discesa.

L'utente può passare alle istruzioni audio selezionando l'icona delle cuffie nella parte inferiore della pagina. La versione audio del puzzle fornisce istruzioni vocali sul testo che l'utente deve digitare in una casella di testo, sovrapposta dal rumore di fondo.

La tabella seguente elenca le lingue che è possibile selezionare per le istruzioni scritte in un puzzle CAPTCHA e il supporto audio per ciascuna selezione.

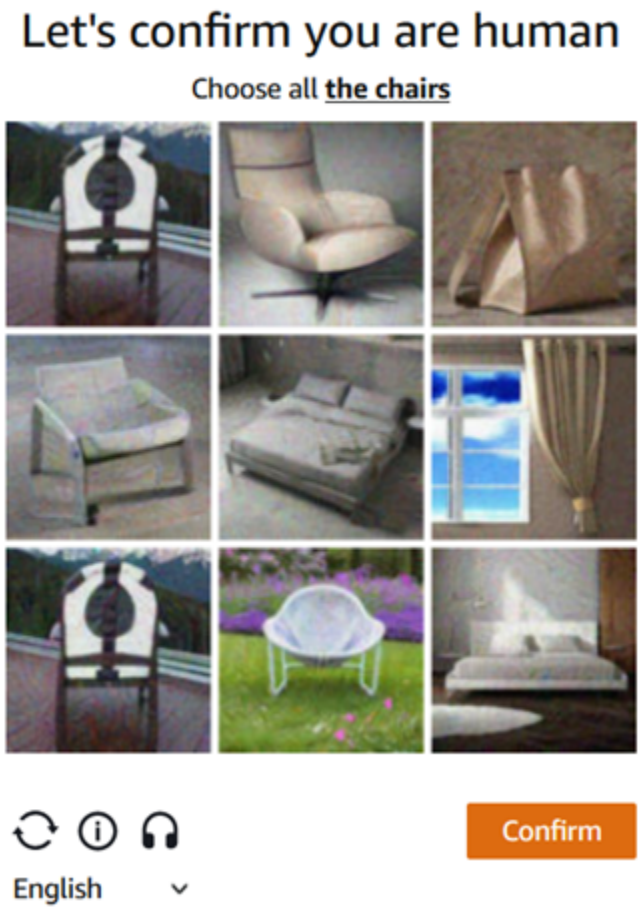
AWS WAF Lingue supportate dai puzzle CAPTCHA

Supporto per istruzioni scritte	Codice locale	Supporto per istruzioni audio
Arabo	ar-SA	Arabo
Cinese semplificato	zh-CN	Audio in inglese
Olandese	nl-NL	Olandese
Italiano	it-IT	Italiano
Francese	fr-FR	Francese
Tedesco	de-DE	Tedesco
Italiano	it-IT	Italiano
Giapponese	ja-JP	Audio in inglese
Portoghese brasiliano	pt-BR	Portoghese brasiliano
Spagnolo	es-ES	Spagnolo
Turco	tr-TR	Turco

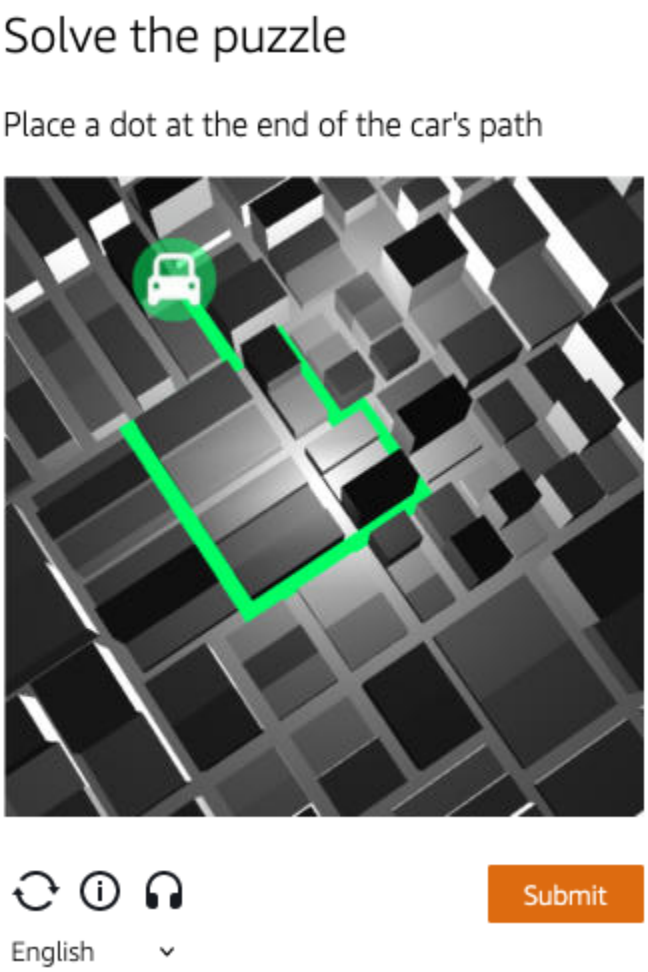
Esempi di puzzle CAPTCHA

Un tipico puzzle CAPTCHA visivo richiede l'interazione per dimostrare che l'utente può comprendere e interagire con una o più immagini.

La schermata seguente mostra un esempio di puzzle a griglia illustrata. Questo puzzle richiede la selezione di tutte le immagini nella griglia che includono un tipo specifico di oggetto.

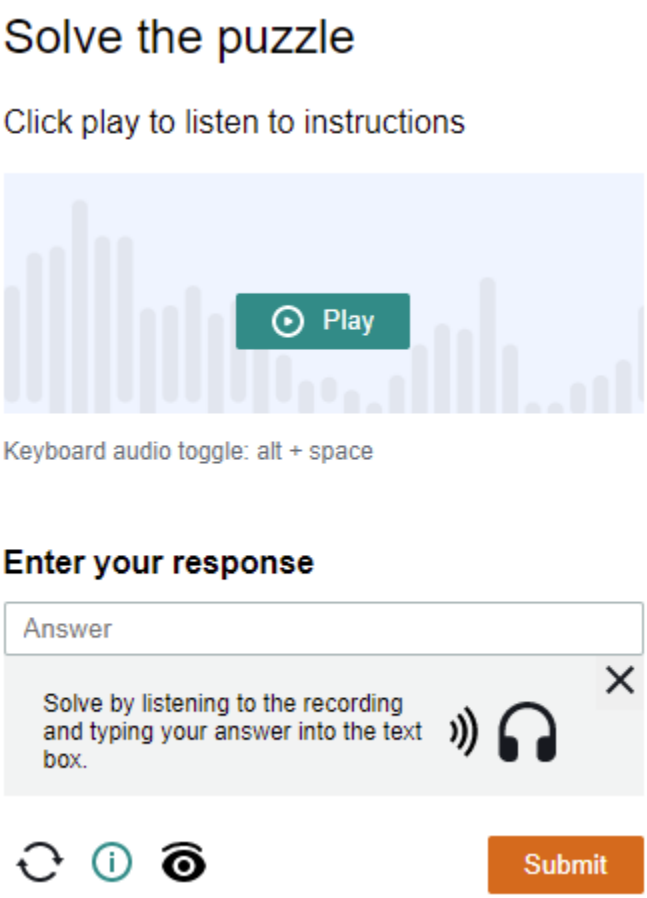


La schermata seguente mostra un esempio di puzzle che richiede di identificare il punto finale del percorso di un'auto in un disegno.



Un rompicapo audio produce un rumore di sottofondo sovrapposto a istruzioni vocali sul testo che l'utente deve digitare in una casella di testo.

La schermata seguente mostra la visualizzazione della scelta del puzzle audio.



Come funzionano le azioni CAPTCHA e le Challenge regole

AWS WAF CAPTCHAe Challenge sono azioni regolate da regole standard, quindi sono relativamente facili da implementare. Per utilizzare entrambe, è necessario creare i criteri di ispezione per la regola che identifica le richieste che si desidera esaminare, quindi specificare una delle due azioni della regola. Per informazioni generali sulle opzioni di azione delle regole, vedere. Operazione delle regole

Oltre a implementare sfide silenziose e puzzle CAPTCHA dal lato server, puoi integrare sfide silenziose nelle tue applicazioni client JavaScript iOS e Android e puoi eseguire il rendering di puzzle CAPTCHA nei tuoi client. JavaScript Queste integrazioni consentono di fornire agli utenti finali prestazioni ed esperienze di puzzle CAPTCHA migliori e possono ridurre i costi associati all'utilizzo delle azioni delle regole e dei gruppi di regole intelligenti per la mitigazione delle minacce. Per ulteriori informazioni su queste opzioni, consulta AWS WAF integrazione delle applicazioni client. Per informazioni sui prezzi, consulta Prezzi di AWS WAF.

Argomenti

CAPTCHAe comportamento Challenge d'azione

Quando una richiesta Web soddisfa i criteri di ispezione di una regola con CAPTCHA o Challenge un'azione, AWS WAF determina come gestire la richiesta in base allo stato del token e alla configurazione del tempo di immunità. AWS WAF valuta anche se la richiesta è in grado di gestire il puzzle CAPTCHA o lo script di sfida interstitial. Gli script sono progettati per essere gestiti come contenuti HTML e possono essere gestiti correttamente solo da un client che prevede contenuti HTML.

> **Note**
>
> Ti vengono addebitati costi aggiuntivi quando utilizzi l'azione CAPTCHA o in una delle tue regole o come Challenge regola che sostituisce un'azione in un gruppo di regole. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.

In che modo l'azione gestisce la richiesta web

AWS WAF applica l'Challengeazione CAPTCHA or a una richiesta web come segue:

- Token valido: la AWS WAF gestisce in modo simile a un'Countazione. AWS WAF applica tutte le etichette e richiede le personalizzazioni che hai configurato per l'azione della regola, quindi continua a valutare la richiesta utilizzando le regole rimanenti nell'ACL web.
- Token mancante, non valido o scaduto: AWS WAF interrompe la valutazione ACL Web della richiesta e ne impedisce l'accesso alla destinazione prevista.

  AWS WAF genera una risposta che invia al client, in base al tipo di azione della regola:

  - Challenge— AWS WAF include quanto segue nella risposta:
    - L'intestazione `x-amzn-waf-action` con un valore di `challenge`.

      > **Note**
      >
      > Questa intestazione non è disponibile per JavaScript le applicazioni eseguite nel browser client. Per i dettagli, consulta la sezione che segue.

    - Codice di stato HTTP `202 Request Accepted`.
    - Se la richiesta contiene un'`Accept`intestazione con un valore di`text/html`, la risposta include una JavaScript pagina interstiziale con uno script di sfida.
- CAPTCHA— AWS WAF include quanto segue nella risposta:
    - L'intestazione `x-amzn-waf-action` con un valore di `captcha`.

      > **Note**
      >
      > Questa intestazione non è disponibile per JavaScript le applicazioni eseguite nel browser client. Per i dettagli, consulta la sezione che segue.

    - Codice di stato HTTP `405 Method Not Allowed`.
    - Se la richiesta contiene un'`Accept`intestazione con un valore di`text/html`, la risposta include una JavaScript pagina interstiziale con uno script CAPTCHA.

Per configurare la tempistica di scadenza dei token a livello di ACL Web o di regola, consulta. Scadenza del timestamp: tempi di immunità dei token

Le intestazioni non sono disponibili per JavaScript le applicazioni eseguite nel browser client

Quando AWS WAF risponde a una richiesta del client con un CAPTCHA o una risposta alla sfida, non include le intestazioni CORS (Cross-Origin Resource Sharing). Le intestazioni CORS sono un insieme di intestazioni per il controllo degli accessi che indicano al browser Web del client quali domini, metodi HTTP e intestazioni HTTP possono essere utilizzati dalle applicazioni. JavaScript Senza le intestazioni CORS, JavaScript le applicazioni in esecuzione in un browser client non hanno accesso alle intestazioni HTTP e quindi non sono in grado di leggere l'`x-amzn-waf-action`intestazione fornita nelle risposte and. CAPTCHA Challenge

A cosa servono gli interstitial Challenge e CAPTCHA

Quando viene eseguita una challenge interstitial, dopo che il client ha risposto con successo, se non dispone già di un token, l'interstitial ne inizializza uno. Quindi aggiorna il token con il timestamp di risoluzione della sfida.

Quando viene eseguito un CAPTCHA interstitial, se il client non ha ancora un token, il CAPTCHA interstitial richiama innanzitutto lo script di sfida per sfidare il browser e inizializzare il token. Quindi l'interstitial esegue il suo puzzle CAPTCHA. Quando l'utente finale completa con successo il puzzle, l'interstitial aggiorna il token con il timestamp di risoluzione CAPTCHA.

In entrambi i casi, dopo che il client ha risposto correttamente e lo script ha aggiornato il token, lo script invia nuovamente la richiesta web originale utilizzando il token aggiornato.

È possibile configurare il modo in cui gestisce i token AWS WAF . Per informazioni, consulta AWS WAF token di richiesta web.

CAPTCHAe Challenge azioni nei log e nelle metriche

Le Challenge azioni CAPTCHA e possono essere non terminantiCount, simili o terminative. Block Il risultato dipende dal fatto che la richiesta abbia un token valido con un timestamp non scaduto per il tipo di azione.

- Token valido: quando l'azione trova un token valido e non blocca la richiesta, AWS WAF acquisisce le metriche e i log come segue:
  - Incrementa le metriche per and o and. `CaptchaRequests` `RequestsWithValidCaptchaToken` `ChallengeRequests` `RequestsWithValidChallengeToken`
  - Registra la partita come `nonTerminatingMatchingRules` immissione con azione di o. CAPTCHA Challenge L'elenco seguente mostra la sezione di un registro relativa a questo tipo di corrispondenza con l'CAPTCHAazione.

```
    "nonTerminatingMatchingRules": [
    {
      "ruleId": "captcha-rule",
      "action": "CAPTCHA",
      "ruleMatchDetails": [],
      "captchaResponse": {
        "responseCode": 0,
        "solveTimestamp": 1632420429
      }
    }
  ]
```

- Token mancante, non valido o scaduto: quando l'azione blocca la richiesta a causa di un token mancante o non valido, AWS WAF acquisisce le metriche e i log come segue:
  - Incrementa la metrica per o. `CaptchaRequests` `ChallengeRequests`
  - Registra la corrispondenza come `CaptchaResponse` voce con codice di `405` stato HTTP o come `ChallengeResponse` voce con codice di stato HTTP`202`. Il registro indica se nella richiesta mancava il token o se aveva un timestamp scaduto. Il registro indica anche se è AWS WAF stata inviata una pagina interstiziale CAPTCHA al client o se è stata inviata una richiesta

silenziosa al browser del client. L'elenco seguente mostra le sezioni di un registro relative a questo tipo di corrispondenza con l'azione. CAPTCHA

```
"terminatingRuleId": "captcha-rule",
"terminatingRuleType": "REGULAR",
"action": "CAPTCHA",
"terminatingRuleMatchDetails": [],
...
"responseCodeSent": 405,
...
"captchaResponse": {
  "responseCode": 405,
  "solveTimestamp": 0,
  "failureReason": "TOKEN_MISSING"
}
```

Per informazioni sui AWS WAF log, vedereRegistrazione del traffico AWS WAF ACL Web.

Per informazioni sulle AWS WAF metriche, consulta. AWS WAF metriche e dimensioni

Per informazioni sulle opzioni di azione delle regole, consultaOperazione delle regole.

Procedure consigliate per l'utilizzo Challenge delle azioni CAPTCHA e

Segui le indicazioni riportate in questa sezione per pianificare e implementare il AWS WAF CAPTCHA o la sfida.

Pianifica il tuo CAPTCHA e sfida l'implementazione

Determina dove posizionare i puzzle CAPTCHA o le sfide silenziose in base all'utilizzo del tuo sito web, alla sensibilità dei dati che desideri proteggere e al tipo di richieste. Seleziona le richieste a cui applicare il CAPTCHA in modo da presentare i puzzle secondo necessità, ma evita di presentarli dove non sarebbero utili e potrebbero compromettere l'esperienza dell'utente. Usa l'Challengeazione per eseguire sfide silenziose che hanno un impatto minore sull'utente finale, ma aiutano comunque a verificare che la richiesta provenga da un browser abilitato. JavaScript

Decidi dove eseguire i puzzle CAPTCHA e le sfide silenziose sui tuoi clienti

Identifica le richieste che non vuoi siano influenzate dal CAPTCHA, ad esempio le richieste di CSS o immagini. Usa CAPTCHA solo quando necessario. Ad esempio, se prevedi di eseguire un controllo CAPTCHA al momento dell'accesso e l'utente passa sempre direttamente dall'accesso a un'altra

schermata, probabilmente non sarebbe necessario richiedere un controllo CAPTCHA nella seconda schermata e potrebbe peggiorare l'esperienza dell'utente finale.

Configura Challenge e CAPTCHA utilizza in modo da inviare AWS WAF solo puzzle CAPTCHA e sfide silenziose in risposta alle richieste. `GET text/html` Non puoi eseguire né il puzzle né la sfida in risposta a `POST` richieste, richieste di preflight Cross-Origin Resource Sharing (CORS) o altri tipi che non contengano `OPTIONS` richieste. `GET` Il comportamento del browser per altri tipi di richieste può variare e potrebbe non essere in grado di gestire correttamente gli interstitial.

È possibile che un client accetti il codice HTML ma non sia comunque in grado di gestire il CAPTCHA o il challenge interstitial. Ad esempio, un widget su una pagina Web con un iFrame di piccole dimensioni potrebbe accettare HTML ma non essere in grado di visualizzare un CAPTCHA o elaborarlo. Evita di inserire le azioni delle regole per questi tipi di richieste, come per le richieste che non accettano HTML.

Utilizza CAPTCHA o Challenge per verificare la precedente acquisizione di token

È possibile utilizzare le azioni delle regole esclusivamente per verificare l'esistenza di un token valido, in luoghi in cui gli utenti legittimi dovrebbero sempre averne uno. In queste situazioni, non importa se la richiesta è in grado di gestire gli interstitial.

Ad esempio, se implementi l'API CAPTCHA dell'applicazione JavaScript client ed esegui il puzzle CAPTCHA sul client immediatamente prima di inviare la prima richiesta all'endpoint protetto, la prima richiesta dovrebbe sempre includere un token valido sia per challenge che per CAPTCHA. Per informazioni sull'integrazione delle applicazioni client, consulta. JavaScript AWS WAF JavaScript integrazioni

In questa situazione, nell'ACL web, puoi aggiungere una regola che corrisponda alla prima chiamata e configurarla con l'azione della CAPTCHA regola Challenge o. Quando la regola corrisponde per un utente finale e un browser legittimi, l'azione troverà un token valido e pertanto non bloccherà la richiesta né invierà una sfida o un puzzle CAPTCHA in risposta. Per ulteriori informazioni su come funzionano le azioni delle regole, consulta. CAPTCHAe comportamento Challenge d'azione

Proteggi i tuoi dati sensibili non HTML con e CAPTCHAChallenge

Puoi utilizzare CAPTCHA e Challenge protezioni per dati sensibili non HTML, come le API, con il seguente approccio.

1. Identifica le richieste che accettano risposte HTML e che vengono eseguite in prossimità delle richieste relative ai tuoi dati sensibili non HTML.

2. Scrivi CAPTCHA o Challenge regole che corrispondano alle richieste di HTML e alle richieste per i tuoi dati sensibili.
3. Ottimizzate le impostazioni relative ai tempi CAPTCHA e alle tempistiche di Challenge immunità in modo che, per le normali interazioni con gli utenti, i token che i client ottengono dalle richieste HTML siano disponibili e non scaduti nelle loro richieste di dati sensibili. Per informazioni sull'ottimizzazione, consulta. Scadenza del timestamp: tempi di immunità dei token

Quando una richiesta di dati sensibili corrisponde a una Challenge regola CAPTCHA or, non verrà bloccata se il client ha ancora un token valido del puzzle o della sfida precedente. Se il token non è disponibile o il timestamp è scaduto, la richiesta di accesso ai dati sensibili avrà esito negativo. Per ulteriori informazioni su come funzionano le azioni delle regole, consulta. CAPTCHAe comportamento Challenge d'azione

Usa CAPTCHA e ottimizza Challenge le regole esistenti

Rivedi le regole esistenti per vedere se desideri modificarle o aggiungerle. Di seguito sono riportati alcuni scenari comuni da considerare.

- Se disponi di una regola basata sulla tariffa che blocca il traffico, ma mantieni il limite di velocità relativamente alto per evitare di bloccare gli utenti legittimi, prendi in considerazione l'aggiunta di una seconda regola basata sulla tariffa dopo la regola di blocco. Assegna alla seconda regola un limite inferiore rispetto alla regola di blocco e imposta l'azione della regola su o. CAPTCHA Challenge La regola di blocco bloccherà comunque le richieste che arrivano a una frequenza troppo elevata e la nuova regola bloccherà la maggior parte del traffico automatizzato a una velocità ancora inferiore. Per informazioni sulle regole basate sulla tariffa, consulta. Istruzione regola basata sulla frequenza
- Se disponi di un gruppo di regole gestito che blocca le richieste, puoi modificare il comportamento di alcune o tutte le regole da o Block aCAPTCHA. Challenge A tale scopo, nella configurazione del gruppo di regole gestito, sovrascrivi l'impostazione dell'azione della regola. Per informazioni sulla sovrascrittura delle azioni delle regole, vedere. L'azione delle regole ha la precedenza

Testa il tuo CAPTCHA e verifica le implementazioni prima di implementarle

Per quanto riguarda tutte le nuove funzionalità, segui le indicazioni riportate all'indirizzo. the section called “Test e messa a punto delle protezioni”

Durante i test, rivedi i requisiti di data e ora di scadenza del token e imposta le configurazioni dell'ACL Web e del tempo di immunità a livello di regola in modo da raggiungere un buon equilibrio

tra il controllo dell'accesso al tuo sito Web e l'offerta di un'esperienza positiva ai tuoi clienti. Per informazioni, consulta Scadenza del timestamp: tempi di immunità dei token.

Registrazione del traffico AWS WAF ACL Web

È possibile attivare la registrazione per ottenere informazioni dettagliate sul traffico analizzato dall'ACL Web. Le informazioni registrate includono l'ora in cui è AWS WAF stata ricevuta una richiesta Web dalla AWS risorsa, informazioni dettagliate sulla richiesta e dettagli sulle regole a cui la richiesta corrisponde. Puoi inviare i log a un gruppo di log Amazon CloudWatch Logs, a un bucket Amazon Simple Storage Service (Amazon S3) o a un Amazon Data Firehose.

> **Note**
>
> La configurazione di registrazione influisce solo sui log. AWS WAF In particolare, la configurazione dei campi oscurati per la registrazione non ha alcun impatto sul campionamento delle richieste. L'unico modo per escludere i campi dalle richieste campionate è disabilitare il campionamento per l'ACL web.

Se non riesci a trovare un record di registro nei tuoi log

In rare occasioni, è possibile che la consegna dei AWS WAF log scenda al di sotto del 100%, con la massima diligenza possibile. L' AWS WAF architettura dà priorità alla sicurezza delle applicazioni rispetto a tutte le altre considerazioni. In alcune situazioni, ad esempio quando i flussi di registrazione subiscono una limitazione del traffico, ciò può comportare la perdita di record. Ciò non dovrebbe influire su più di alcuni record. Se noti una serie di voci di registro mancanti, contatta il AWS Support Centro.

Argomenti

- Prezzi per la registrazione delle informazioni sul traffico ACL Web
- AWS WAF destinazioni di registrazione
- Gestione della registrazione per un ACL Web
- Campi di log
- Esempi di log

Prezzi per la registrazione delle informazioni sul traffico ACL Web

La registrazione delle informazioni sul traffico Web ACL viene addebitata in base ai costi associati a ciascun tipo di destinazione del registro. Questi costi si aggiungono ai costi di utilizzo. AWS WAF I costi possono variare in base a fattori quali il tipo di destinazione scelto e la quantità di dati registrati.

Di seguito sono riportati i collegamenti alle informazioni sui prezzi per ogni tipo di destinazione di registrazione:

- CloudWatch Registri: i costi si riferiscono alla consegna dei registri venduti. Consulta i prezzi di Amazon CloudWatch Logs. In Livello a pagamento, scegli la scheda Logs, quindi in Vending Logs, consulta le informazioni per Delivery to Logs. CloudWatch
- Bucket Amazon S3: i costi di Amazon S3 sono i costi combinati per la consegna di CloudWatch log in vendita ai bucket Amazon S3 e per l'utilizzo di Amazon S3.
  - Per Amazon S3, consulta i prezzi di Amazon S3.
  - Per la consegna CloudWatch dei log in vendita ad Amazon S3, consulta i prezzi di Amazon Logs. CloudWatch In Livello a pagamento, scegli la scheda Logs, quindi in Vending Logs, consulta le informazioni per la consegna a S3
- Firehose: consulta i prezzi di Amazon Data Firehose.

Per informazioni sui AWS WAF prezzi, consulta AWS WAF la pagina Prezzi.

AWS WAF destinazioni di registrazione

Questa sezione descrive le opzioni di registrazione tra cui scegliere per i log. AWS WAF Ogni sezione fornisce indicazioni per la configurazione della registrazione, incluse informazioni su qualsiasi comportamento specifico del tipo di destinazione. Dopo aver configurato la destinazione di registrazione, è possibile fornire le relative specifiche alla configurazione di registrazione ACL Web per iniziare la registrazione.

Argomenti

- CloudWatch Registri Amazon
- Amazon Simple Storage Service
- Amazon Data Firehose

CloudWatch Registri Amazon

Questo argomento fornisce informazioni per inviare i log di traffico Web ACL a un gruppo di log Logs. CloudWatch

> **Note**
>
> Oltre ai costi di utilizzo, ti verranno addebitati i costi per la registrazione. AWS WAF Per informazioni, consulta Prezzi per la registrazione delle informazioni sul traffico ACL Web.

Per inviare i log ad Amazon CloudWatch Logs, devi creare un gruppo di CloudWatch log Logs. Quando si abilita l'accesso AWS WAF, si fornisce l'ARN del gruppo di log. Dopo aver abilitato la registrazione per l'ACL Web, AWS WAF invia i log al gruppo Logs log nei flussi di CloudWatch log.

Quando usi CloudWatch Logs, puoi esplorare i log del tuo ACL web nella console. AWS WAF Nella tua pagina web ACL, seleziona la scheda Logging insights. Questa opzione si aggiunge alle informazioni di registrazione fornite per i CloudWatch registri tramite la console. CloudWatch

Configura il gruppo di log per i registri ACL AWS WAF Web nella stessa regione dell'ACL Web e utilizza lo stesso account utilizzato per gestire l'ACL Web. Per informazioni sulla configurazione di un gruppo di log CloudWatch Logs, consultate Working with Log Groups and Log Streams.

Quote per i gruppi di log Logs CloudWatch

CloudWatch Logs ha una quota massima predefinita per la velocità effettiva, condivisa tra tutti i gruppi di log all'interno di una regione, che è possibile richiedere di aumentare. Se i tuoi requisiti di registrazione sono troppo elevati per l'attuale impostazione del throughput, vedrai le metriche di limitazione relative al tuo account. `PutLogEvents` Per visualizzare il limite nella console Service Quotas e richiedere un aumento, consulta la quota CloudWatch PutLogEvents Logs.

Denominazione dei gruppi di log

I nomi dei gruppi di log devono iniziare con `aws-waf-logs-` e possono terminare con qualsiasi suffisso desiderato, ad esempio. `aws-waf-logs-testLogGroup2`

Il formato ARN risultante è il seguente:

```
arn:aws:logs:Region:account-id:log-group:aws-waf-logs-log-group-suffix
```

I flussi di log hanno il seguente formato di denominazione:

```
Region_web-acl-name_log-stream-number
```

Di seguito viene illustrato un esempio di flusso di log per l'ACL `TestWebACL` Web in Region. `us-east-1`

```
us-east-1_TestWebACL_0
```

Autorizzazioni necessarie per pubblicare i log in Logs CloudWatch

La configurazione della registrazione del traffico Web ACL per un gruppo di log CloudWatch Logs richiede le impostazioni di autorizzazione descritte in questa sezione. Le autorizzazioni vengono impostate automaticamente quando si utilizza una delle politiche di accesso gestito AWS WAF completo, oppure. `AWSWAFConsoleFullAccess` `AWSWAFFullAccess` Se desideri gestire un accesso più dettagliato alla registrazione e alle AWS WAF risorse, puoi impostare tu stesso le autorizzazioni. Per informazioni sulla gestione delle autorizzazioni, consulta Gestione degli accessi alle AWS risorse nella Guida per l'utente IAM. Per informazioni sulle politiche AWS WAF gestite, consultaAWS politiche gestite per AWS WAF.

Queste autorizzazioni consentono di modificare la configurazione della registrazione Web ACL, di configurare la consegna dei log per CloudWatch i registri e di recuperare informazioni sul gruppo di log. Queste autorizzazioni devono essere associate all'utente che utilizzi per la gestione. 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"
      }
   ]
}
```

Quando sono consentite azioni su tutte AWS le risorse, ciò è indicato nella politica con un'`"Resource"`impostazione di`"*"`. Ciò significa che le azioni sono consentite su tutte le AWS risorse supportate da ciascuna azione. Ad esempio, l'azione `wafv2:PutLoggingConfiguration` è supportata solo per la `wafv2` registrazione delle risorse di configurazione.

Amazon Simple Storage Service

Questo argomento fornisce informazioni per inviare i log di traffico ACL Web a un bucket Amazon S3.

> **Note**
>
> Oltre ai costi di utilizzo, ti verranno addebitati i costi per la registrazione. AWS WAF Per informazioni, consulta Prezzi per la registrazione delle informazioni sul traffico ACL Web.

Per inviare i log del traffico Web ACL ad Amazon S3, è necessario configurare un bucket Amazon S3 dallo stesso account utilizzato per gestire l'ACL Web e assegnare un nome al bucket a partire da. `aws-waf-logs-` Quando abiliti l'accesso, fornisci il nome del bucket. AWS WAF Per informazioni sulla creazione di un bucket di registrazione, consulta Create a Bucket nella Amazon Simple Storage Service User Guide.

Puoi accedere e analizzare i log di Amazon S3 utilizzando il servizio di query interattivo Amazon Athena. Athena semplifica l'analisi dei dati direttamente in Amazon S3 utilizzando SQL standard. Con poche azioni AWS Management Console, puoi indirizzare Athena ai tuoi dati archiviati in Amazon S3

e iniziare rapidamente a utilizzare SQL standard per eseguire query ad hoc e ottenere risultati. Per ulteriori informazioni, consulta la sezione Interrogazione dei AWS WAF log nella guida per l'utente di Amazon Athena.

> **Note**
>
> AWS WAF supporta la crittografia con bucket Amazon S3 per il tipo di chiave Amazon S3 key (SSE-S3) e per (SSE-KMS). AWS Key Management Service AWS KMS keys AWS WAF non supporta la crittografia per le chiavi gestite da. AWS Key Management Service AWS

I tuoi ACL Web pubblicano i propri file di log nel bucket Amazon S3 a intervalli di 5 minuti. Ogni file di registro contiene i record di registro per il traffico registrato nei 5 minuti precedenti.

Le dimensioni file massime per un file di log sono di 75 MB. Se il file di registro raggiunge il limite di dimensione del file entro un periodo di 5 minuti, interrompe l'aggiunta di record, lo pubblica nel bucket Amazon S3 e quindi crea un nuovo file di registro.

I file di log sono compressi. Se apri i file utilizzando la console Amazon S3, Amazon S3 decomprime i record di log e li visualizza. Se scarichi i file di registro, devi decomprimerli per visualizzare i record.

Un singolo file di registro contiene voci interlacciate con più record. Per visualizzare tutti i file di registro di un ACL Web, cerca le voci aggregate in base al nome ACL Web, alla regione e all'ID dell'account.

Requisiti di denominazione e sintassi

I nomi dei bucket per la AWS WAF registrazione devono iniziare con `aws-waf-logs-` e possono terminare con qualsiasi suffisso che desideri. Ad esempio, `aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX`.

Posizione del bucket

Le posizioni dei bucket utilizzano la seguente sintassi:

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/
```

Bucket ARN

Il formato del bucket Amazon Resource Name (ARN) è il seguente:

```
arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX
```

Posizioni dei bucket con prefissi

Se utilizzi prefissi nel nome delle chiavi oggetto per organizzare i dati archiviati nei bucket, puoi fornire i prefissi nei nomi dei bucket di registrazione.

> **Note**
>
> Questa opzione non è disponibile tramite la console. Usa le AWS WAF API, la CLI o. AWS CloudFormation

Per informazioni sull'uso dei prefissi in Amazon S3, consulta Organizing objects using prefixes nella Amazon Simple Storage Service User Guide.

Le posizioni dei bucket con prefissi utilizzano la seguente sintassi:

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/DOC-EXAMPLE-KEY-NAME-PREFIX/
```

Cartelle e nomi di file dei bucket

All'interno dei bucket e seguendo i prefissi che fornisci, AWS WAF i log sono scritti in una struttura di cartelle determinata dall'ID dell'account, dalla regione, dal nome ACL web e dalla data e dall'ora.

```
AWSLogs/account-id/WAFLogs/Region/web-acl-name/YYYY/MM/dd/HH/mm
```

All'interno delle cartelle, i nomi dei file di registro seguono un formato simile:

```
account-id_waflogs_Region_web-acl-name_timestamp_hash.log.gz
```

Le specifiche temporali utilizzate nella struttura delle cartelle e nel nome del file di registro rispettano le specifiche del formato del timestamp. `YYYYMMddTHHmmZ`

Di seguito viene illustrato un esempio di file di log in un bucket Amazon S3 per un bucket denominato. `DOC-EXAMPLE-BUCKET` Lo è. Account AWS `11111111111` L'ACL web è `TEST-WEBACL` e la regione è`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**
>
> I nomi dei bucket per la AWS WAF registrazione devono iniziare con `aws-waf-logs-` e possono terminare con qualsiasi suffisso desiderato.

Autorizzazioni necessarie per pubblicare i log su Amazon S3

La configurazione della registrazione del traffico Web ACL per un bucket Amazon S3 richiede le seguenti impostazioni di autorizzazione. Queste autorizzazioni vengono impostate automaticamente quando utilizzi una delle politiche di gestione dell'accesso completo, oppure. AWS WAF `AWSWAFConsoleFullAccess` `AWSWAFFullAccess` Se desideri gestire un accesso più dettagliato alla registrazione e alle AWS WAF risorse, puoi impostare tu stesso queste autorizzazioni. Per informazioni sulla gestione delle autorizzazioni, consulta Gestione degli accessi alle AWS risorse nella Guida per l'utente IAM. Per informazioni sulle politiche AWS WAF gestite, consultaAWS politiche gestite per AWS WAF.

Le seguenti autorizzazioni consentono di modificare la configurazione di registrazione ACL Web e di configurare la consegna dei log al bucket Amazon S3. Queste autorizzazioni devono essere associate all'utente che utilizzi per la gestione. AWS WAF

> **Note**
>
> Quando imposti le autorizzazioni elencate di seguito, potresti visualizzare errori nei AWS CloudTrail registri che indicano un accesso negato, ma le autorizzazioni sono corrette per la registrazione. AWS WAF

```
{
   "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-example-bucket"
         ],
         "Effect":"Allow"
      }
   ]
}
```

Quando sono consentite azioni su tutte le AWS risorse, ciò è indicato nella politica con un'impostazione di. `"Resource" "*"` Ciò significa che le azioni sono consentite su tutte le AWS risorse supportate da ciascuna azione. Ad esempio, l'azione `wafv2:PutLoggingConfiguration` è supportata solo per la `wafv2` registrazione delle risorse di configurazione.

Per impostazione predefinita, i bucket Amazon S3 e gli oggetti che contengono sono privati. Solo il proprietario del bucket può accedere al bucket e agli oggetti in esso archiviati. Il proprietario del bucket, tuttavia, può concedere l'accesso ad altre risorse e utenti scrivendo una politica di accesso.

Se l'utente che crea il log è proprietario del bucket, il servizio allega automaticamente la seguente policy al bucket per concedere al log l'autorizzazione a pubblicare i log su di esso:

```
{
  "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-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-example-bucket",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": ["account-id"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
        }
```

```
      }
    }
  ]
}
```

> **Note**
>
> I nomi dei bucket per la AWS WAF registrazione devono iniziare con `aws-waf-logs-` e possono terminare con qualsiasi suffisso desiderato.

Se l'utente che crea il log non è proprietario del bucket o non dispone delle autorizzazioni `GetBucketPolicy` e dei `PutBucketPolicy` permessi per il bucket, la creazione del log ha esito negativo. In questo caso, il proprietario del bucket deve aggiungere manualmente la politica precedente al bucket e specificare l'ID del creatore del log. Account AWS Per ulteriori informazioni, consulta Come aggiungere una policy per un bucket S3 nella Guida per l'utente di Amazon Simple Storage Service. Se il bucket riceve log da più account, aggiungi un `Resource` elemento all'`AWSLogDeliveryWrite`informativa relativa a ciascun account.

Ad esempio, la seguente politica sui bucket consente di Account AWS `111122223333` pubblicare i log in un bucket denominato: `aws-waf-logs-doc-example`

```
{
    "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-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-example-bucket",
            "Condition": {
                "StringEquals": {
                "aws:SourceAccount": ["111122223333"]
                },
                "ArnLike": {
                "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
                }
            }
        }
    ]
}
```

Autorizzazioni per l'utilizzo con una chiave KMS AWS Key Management Service

Se la destinazione di registrazione utilizza la crittografia lato server con chiavi archiviate in AWS Key Management Service (SSE-KMS) e utilizzi una chiave gestita dal cliente (chiave KMS), devi autorizzare l'uso della tua chiave KMS. AWS WAF A tale scopo, aggiungi una politica chiave alla chiave KMS per la destinazione scelta. Ciò consente la AWS WAF registrazione per scrivere i file di registro nella destinazione.

Aggiungi la seguente policy chiave alla tua chiave KMS per consentire l'accesso AWS WAF al tuo bucket Amazon S3.

```
{
    "Sid": "Allow AWS WAF to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
```

```
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*"
}
```

Autorizzazioni necessarie per accedere ai file di registro di Amazon S3

Amazon S3 utilizza le liste di controllo degli accessi (ACL) per gestire l'accesso ai file di registro creati da un registro. AWS WAF Per impostazione predefinita, il proprietario del bucket dispone di autorizzazioni `FULL_CONTROL` su ogni file di log. Il proprietario della distribuzione dei log, se diverso dal proprietario del bucket, non dispone di autorizzazioni. L'account di distribuzione dei log dispone delle autorizzazioni `READ` e `WRITE`. Per ulteriori informazioni, consulta Panoramica della lista di controllo accessi nella Guida per l'utente di Amazon Simple Storage Service.

Amazon Data Firehose

Questa sezione fornisce informazioni per inviare i log di traffico ACL Web a un Amazon Data Firehose.

> **Note**
>
> Oltre ai costi di utilizzo, ti verranno addebitati i costi per la registrazione. AWS WAF Per informazioni, consulta Prezzi per la registrazione delle informazioni sul traffico ACL Web.

Per inviare i log ad Amazon Data Firehose, devi inviare i log dal tuo ACL Web a un Amazon Data Firehose con una destinazione di storage configurata. Dopo aver abilitato la registrazione, AWS WAF invia i log alla destinazione di archiviazione tramite l'endpoint HTTPS di Firehose.

Un AWS WAF registro equivale a un record Firehose. Se in genere ricevi 10.000 richieste al secondo e abiliti i log completi, dovresti avere un'impostazione di 10.000 record al secondo in Firehose. Se non configuri Firehose correttamente, AWS WAF non registrerà tutti i log. Per ulteriori informazioni, consulta Quote di Amazon Kinesis Data Firehose.

Per informazioni su come creare un Amazon Data Firehose e rivedere i log memorizzati, consulta What Is Amazon Data Firehose?

Per informazioni sulla creazione di un flusso di distribuzione, consulta Creating an Amazon Data Firehose Delivery Stream.

Configurazione di un flusso di distribuzione Amazon Data Firehose per il tuo ACL web

Configura un flusso di distribuzione Amazon Data Firehose per il tuo ACL web come segue.

- Crealo utilizzando lo stesso account che usi per gestire l'ACL web.
- Crealo nella stessa regione dell'ACL web. Se stai acquisendo log per Amazon CloudFront, crea il firehose nella regione Stati Uniti orientali (Virginia settentrionale),. `us-east-1`
- Assegna al data firehose un nome che inizi con il prefisso. `aws-waf-logs-` Ad esempio, `aws-waf-logs-us-east-2-analytics`.
- Configuralo per l'immissione diretta, che consente alle applicazioni di accedere direttamente al flusso di distribuzione. Nella console Amazon Data Firehose, per l'impostazione della sorgente del flusso di distribuzione, scegli Direct PUT o altre fonti. Tramite l'API, imposta la proprietà del flusso di consegna `DeliveryStreamType` su`DirectPut`.

> **Note**
>
> Non utilizzare a `Kinesis stream` come fonte.

Autorizzazioni necessarie per pubblicare i log su Amazon Data Firehose

Per comprendere le autorizzazioni richieste per la configurazione di Kinesis Data Firehose, consulta Controlling Access with Amazon Kinesis Data Firehose.

È necessario disporre delle seguenti autorizzazioni per abilitare correttamente la registrazione ACL Web con Amazon Data Firehose.

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

Per informazioni sui ruoli collegati ai servizi e sull'autorizzazione, consulta. `iam:CreateServiceLinkedRole` Utilizzo di ruoli collegati ai servizi per AWS WAF

Gestione della registrazione per un ACL Web

È possibile abilitare e disabilitare la registrazione per un ACL Web in qualsiasi momento.

> **Note**
>
> Oltre ai costi di utilizzo, ti verranno addebitati i costi per la registrazione. AWS WAF Per informazioni, consulta Prezzi per la registrazione delle informazioni sul traffico ACL Web.

Nella configurazione di registrazione per il tuo ACL web, puoi personalizzare ciò che AWS WAF viene inviato ai log.

- Redazione dei campi: è possibile oscurare i seguenti campi dai record di registro per le regole che utilizzano le impostazioni di corrispondenza corrispondenti: percorso URI, stringa di query, intestazione singola e metodo HTTP. I campi oscurati vengono visualizzati come `REDACTED` nei log. Ad esempio, se si oscura il campo Query string, nei log, verrà elencato come `REDACTED` per tutte le regole che utilizzano l'impostazione del componente Query string match. La redazione si applica solo al componente di richiesta specificato per la corrispondenza nella regola, quindi la redazione del componente Single header non si applica alle regole che corrispondono nelle intestazioni. Per un elenco dei campi di registro, vedi. Campi di log

  > **Note**
  >
  > Questa impostazione non ha alcun impatto sul campionamento delle richieste. Con il campionamento su richiesta, l'unico modo per escludere i campi è disabilitare il campionamento per l'ACL Web.

- Filtraggio dei log: è possibile aggiungere filtri per specificare quali richieste Web vengono conservate nei log e quali vengono eliminate. Si filtra in base alle impostazioni che AWS WAF si applicano durante la valutazione delle richieste Web. È possibile filtrare in base alle seguenti impostazioni:
  - Etichetta completamente qualificata: le etichette completamente qualificate hanno un prefisso, namespace opzionali e nome dell'etichetta. Il prefisso identifica il gruppo di regole o il contesto ACL web della regola che ha aggiunto l'etichetta. Per informazioni sulle etichette, vedere. AWS WAF etichette sulle richieste web
  - Azione delle regole: è possibile filtrare in base a qualsiasi normale impostazione di azione delle regole e anche in base all'opzione di `EXCLUDED_AS_COUNT` sostituzione precedente per le regole dei gruppi di regole. Per informazioni sulle impostazioni delle azioni delle regole, vedereOperazione delle regole. Per informazioni sulle regole correnti e precedenti che sostituiscono le regole dei gruppi di regole, vedere. Le azioni sostituiscono i gruppi di regole

- I normali filtri di azione delle regole si applicano alle azioni configurate nelle regole e anche alle azioni configurate utilizzando l'opzione corrente per sovrascrivere un'azione delle regole del gruppo di regole.
- Il filtro di `EXCLUDED_AS_COUNT` registro si sovrappone al filtro del registro delle `Count` azioni. `EXCLUDED_AS_COUNT`filtra sia le opzioni correnti che quelle precedenti per sovrascrivere l'azione di una regola di un gruppo di regole. Count

Per attivare la registrazione per un ACL Web

Questa procedura richiede una destinazione di registrazione configurata. Per informazioni sulle scelte di destinazione e sui requisiti per ciascuna di esse, consultaAWS WAF destinazioni di registrazione.

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).
3. Scegli il nome dell'ACL web per cui desideri abilitare la registrazione. La console consente di accedere alla descrizione dell'ACL Web, dove è possibile modificarla.
4. Nella scheda Logging (Registrazione), selezionare Enable logging (Attiva registrazione).
5. Scegli il tipo di destinazione di registrazione, quindi scegli la destinazione di registrazione che hai configurato. È necessario scegliere una destinazione di registrazione il cui nome inizi con. `aws-waf-logs-`
6. (Facoltativo) Se non desideri che alcuni campi siano inclusi nei registri, modificali. Scegliere il campo da omettere, quindi selezionare Add (Aggiungi). Se necessario, ripetere l'operazione per omettere i campi aggiuntivi.

   > **Note**
   >
   > Questa impostazione non ha alcun impatto sul campionamento delle richieste. Con il campionamento su richiesta, l'unico modo per escludere i campi è disabilitare il campionamento per l'ACL Web.

7. (Facoltativo) Se non desideri inviare tutte le richieste ai log, aggiungi i criteri e il comportamento di filtro. In Filtra log, per ogni filtro che desideri applicare, scegli Aggiungi filtro, quindi scegli i criteri di filtro e specifica se desideri conservare o eliminare le richieste che corrispondono ai criteri. Al termine dell'aggiunta dei filtri, se necessario, modifica il comportamento di registrazione predefinito.

8. Scegliere Enable Logging (Attiva registrazione).

> **Note**
>
> Quando abiliti correttamente la registrazione, AWS WAF creerà un ruolo collegato al servizio con le autorizzazioni necessarie per scrivere i log nella destinazione di registrazione. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AWS WAF.

Per disabilitare la registrazione per un ACL Web

1. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).
2. Scegli il nome dell'ACL web per cui desideri disabilitare la registrazione. La console consente di accedere alla descrizione dell'ACL Web, dove è possibile modificarla.
3. Nella scheda Logging (Registrazione), selezionare Disable logging (Disabilita registrazione).
4. Nella finestra di dialogo, selezionare Disable logging (Disabilita registrazione).

Campi di log

L'elenco seguente descrive i possibili campi di registro.

action

L'azione di terminazione AWS WAF applicata alla richiesta. Ciò indica l'autorizzazione, il blocco, il CAPTCHA o la contestazione. Le Challenge azioni CAPTCHA and terminano quando la richiesta web non contiene un token valido.

args

Stringa query.

Risposta CAPTCHA

Lo stato dell'azione CAPTCHA per la richiesta, compilato quando viene applicata un'CAPTCHAazione alla richiesta. Questo campo viene compilato per qualsiasi CAPTCHA azione, terminante o non terminante. Se una richiesta ha l'CAPTCHAazione applicata più volte, questo campo viene compilato dall'ultima volta che l'azione è stata applicata.

L'CAPTCHAazione interrompe l'ispezione delle richieste Web quando la richiesta non include un token o il token non è valido o è scaduto. Se l'CAPTCHAazione sta terminando, questo campo include un codice di risposta e il motivo dell'errore. Se l'azione non è terminativa, questo campo include un timestamp di risoluzione. Per distinguere tra un'azione terminante e un'azione non terminante, puoi filtrare in base a un attributo non vuoto in questo campo. `failureReason`

Risposta alla sfida

Lo stato dell'azione di sfida per la richiesta, compilato quando un'Challengeazione viene applicata alla richiesta. Questo campo viene compilato per qualsiasi Challenge azione, terminante o non terminante. Se una richiesta ha l'Challengeazione applicata più volte, questo campo viene compilato dall'ultima volta che l'azione è stata applicata.

L'Challengeazione interrompe l'ispezione delle richieste Web quando la richiesta non include un token o il token non è valido o è scaduto. Se l'Challengeazione sta terminando, questo campo include un codice di risposta e il motivo dell'errore. Se l'azione non è terminativa, questo campo include un timestamp di risoluzione. Per distinguere tra un'azione terminante e un'azione non terminante, puoi filtrare in base a un attributo non vuoto in questo campo. `failureReason`

clientIp

Indirizzo IP del client che invia la richiesta.

country

Paese di origine della richiesta. Se non AWS WAF è in grado di determinare il paese di origine, imposta questo campo su. -

excludedRules

Utilizzato solo per le regole dei gruppi di regole. L'elenco di regole nel gruppo di regole che sono state escluse. L'azione per queste regole è impostata suCount.

Se sostituisci una regola per contarla utilizzando l'opzione di azione sostituisci la regola, le corrispondenze non vengono elencate qui. Sono elencate come coppie `action` di azioni e. `overriddenAction`

exclusionType

Un tipo che indica che la regola esclusa ha l'azione. Count

ruleId

L'ID della regola all'interno del gruppo di regole che è esclusa.

Tipo di formato

Tipo di formato per il log.

headers

Elenco intestazioni.

httpMethod

Metodo HTTP nella richiesta.

httpRequest

Metadati sulla richiesta.

httpSourceId

L'ID della risorsa associata:

- Per una CloudFront distribuzione Amazon, l'ID è il seguente *`distribution-id`* nella sintassi ARN:

  `arn:`*`partition`*`cloudfront::`*`account-id`*`:distribution/`*`distribution-id`*

- Per un Application Load Balancer, l'ID è il seguente *`load-balancer-id`* nella sintassi ARN:

  `arn:`*`partition`*`:elasticloadbalancing:`*`region`*`:`*`account-id`*`:loadbalancer/app/`*`load-balancer-name/load-balancer-id`*

- Per un'API REST di Amazon API Gateway, l'ID è il *`api-id`* seguente nella sintassi ARN:

  `arn:`*`partition`*`:apigateway:`*`region`*`::/restapis/`*`api-id`*`/stages/`*`stage-name`*

- Per un'API AWS AppSync GraphQL, l'ID è il seguente *`GraphQLApiId`* nella sintassi ARN:

  `arn:`*`partition`*`:appsync:`*`region`*`:`*`account-id`*`:apis/`*`GraphQLApiId`*

- Per un pool di utenti di Amazon Cognito, l'ID è il seguente *`user-pool-id`* nella sintassi ARN:

  `arn:`*`partition`*`:cognito-idp:`*`region`*`:`*`account-id`*`:userpool/`*`user-pool-id`*

- Per un AWS App Runner servizio, l'ID è il seguente *`apprunner-service-id`* nella sintassi ARN:

  `arn:`*`partition`*`:apprunner:`*`region`*`:`*`account-id`*`:service/`*`apprunner-service-name/apprunner-service-id`*

httpSourceName

Origine della richiesta. Valori possibili: `CF` per Amazon CloudFront, `APIGW` per Amazon API Gateway, `ALB` per Application Load Balancer, `APPSYNC` per Amazon Cognito AWS AppSync`APPRUNNER`, `COGNITOIDP` per App Runner e per Verified Access. `VERIFIED_ACCESS`

httpVersion

Versione HTTP.

Impronta digitale JA3

L'impronta digitale JA3 della richiesta. L'impronta digitale JA3 è un hash di 32 caratteri derivato dal TLS Client Hello di una richiesta in arrivo. Questa impronta digitale funge da identificatore univoco per la configurazione TLS del client. AWS WAF calcola e registra questa impronta digitale per ogni richiesta che contiene informazioni TLS Client Hello sufficienti per il calcolo.

Fornisci questo valore quando configuri una corrispondenza di impronte digitali JA3 nelle tue regole ACL web. Per informazioni sulla creazione di una corrispondenza con l'impronta digitale JA3, vedi Impronta digitale JA3 nella dichiarazione per una regola. Richiedi le opzioni dei componenti

labels

Le etichette sulla richiesta web. Queste etichette sono state applicate in base a regole utilizzate per valutare la richiesta. AWS WAF registra le prime 100 etichette.

nonTerminatingMatchingRegole

L'elenco delle regole non terminative che corrispondono alla richiesta. Ogni elemento dell'elenco contiene le seguenti informazioni.

action

L'azione AWS WAF applicata alla richiesta. Indica il conteggio, il CAPTCHA o la sfida. Gli CAPTCHA e Challenge non terminano quando la richiesta web contiene un token valido.

ruleId

L'ID della regola che corrispondeva alla richiesta e non terminava.

ruleMatchDetails

Informazioni dettagliate sulla regola corrispondente alla richiesta. Questo campo viene compilato solo per le istruzioni SQL injection e Cross-Site Scripting (XSS) Match Rule. Una

regola di corrispondenza potrebbe richiedere una corrispondenza per più di un criterio di ispezione, pertanto questi dettagli di corrispondenza vengono forniti come una serie di criteri di corrispondenza.

Le eventuali informazioni aggiuntive fornite per ciascuna regola variano in base a fattori quali la configurazione della regola, il tipo di corrispondenza delle regole e i dettagli della corrispondenza. Ad esempio, per le regole con un'Challengeazione CAPTCHA o, `challengeResponse` verrà elencato l'`captchaResponse`o. Se la regola corrispondente fa parte di un gruppo di regole e hai sovrascritto l'azione della regola configurata, l'azione configurata verrà fornita in. `overriddenAction`

Campi sovradimensionati

L'elenco dei campi della richiesta Web che sono stati controllati dall'ACL Web e che superano il limite di ispezione. AWS WAF Se un campo è sovradimensionato ma l'ACL web non lo ispeziona, non verrà elencato qui.

Questo elenco può contenere zero o più dei seguenti valori:`REQUEST_BODY`,`REQUEST_JSON_BODY`, `REQUEST_HEADERS` e. `REQUEST_COOKIES` Per ulteriori informazioni sui campi sovradimensionati, vedereGestione di componenti di richieste Web di grandi dimensioni in AWS WAF.

rateBasedRuleElenco

Elenco dei gruppi di regole basate su tariffa che hanno operato su questa richiesta. Per informazioni sulle regole basate sulle tariffe, vedere. Istruzione regola basata sulla frequenza

rateBasedRuleId

ID della regola basata sulla frequenza che ha operato su questa richiesta. Se ciò ha terminato la richiesta, l'ID di `rateBasedRuleId` è uguale all'ID di `terminatingRuleId`.

rateBasedRuleNome

Il nome della regola basata sulla tariffa che ha funzionato sulla richiesta.

limitKey

Il tipo di aggregazione utilizzato dalla regola. I valori possibili sono `IP` per l'origine della richiesta Web, `FORWARDED_IP` per un IP inoltrato in un'intestazione della richiesta, `CUSTOMKEYS` per le impostazioni di chiave aggregate personalizzate e `CONSTANT` per contare tutte le richieste insieme, senza aggregazione.

Valore limite

Utilizzato solo per limitare la velocità in base a un singolo tipo di indirizzo IP. Se una richiesta contiene un indirizzo IP non valido, lo `limitvalue` è`INVALID`.

maxRateAllowed

Il numero massimo di richieste consentite nella finestra temporale specificata per una specifica istanza di aggregazione. L'istanza di aggregazione è definita dalla `limitKey` somma di eventuali specifiche chiave aggiuntive fornite nella configurazione delle regole basate sulla frequenza.

evaluationWindowSec

La quantità di tempo AWS WAF inclusa nella richiesta conta, in secondi.

Valori personalizzati

Valori univoci identificati dalla regola basata sulla tariffa nella richiesta. Per i valori di stringa, i registri stampano i primi 32 caratteri del valore della stringa. A seconda del tipo di chiave, questi valori potrebbero essere solo per una chiave, ad esempio per il metodo HTTP o la stringa di query, oppure potrebbero riguardare una chiave e un nome, ad esempio per l'intestazione e il nome dell'intestazione.

requestHeadersInserted

L'elenco delle intestazioni inserite per la gestione personalizzata delle richieste.

requestId

ID della richiesta, generato dal servizio host sottostante. Per Application Load Balancer, questo è l'ID di traccia. Per tutti gli altri, questo è l'ID della richiesta.

responseCodeSent

Il codice di risposta inviato con una risposta personalizzata.

ruleGroupId

ID del gruppo di regole. Se la regola ha bloccato la richiesta, l'ID per `ruleGroupID` è uguale all'ID per `terminatingRuleId`.

ruleGroupList

L'elenco dei gruppi di regole che hanno risposto a questa richiesta, con informazioni sulla corrispondenza.

terminatingRule

La regola che ha terminato la richiesta. Se è presente, contiene le seguenti informazioni.

action

L'azione di terminazione AWS WAF applicata alla richiesta. Ciò indica l'autorizzazione, il blocco, il CAPTCHA o la contestazione. Le Challenge azioni CAPTCHA and terminano quando la richiesta web non contiene un token valido.

ruleId

L'ID della regola che corrisponde alla richiesta.

ruleMatchDetails

Informazioni dettagliate sulla regola corrispondente alla richiesta. Questo campo viene compilato solo per le istruzioni SQL injection e Cross-Site Scripting (XSS) Match Rule. Una regola di corrispondenza potrebbe richiedere una corrispondenza per più di un criterio di ispezione, pertanto questi dettagli di corrispondenza vengono forniti come una serie di criteri di corrispondenza.

Le eventuali informazioni aggiuntive fornite per ciascuna regola variano in base a fattori quali la configurazione della regola, il tipo di corrispondenza delle regole e i dettagli della corrispondenza. Ad esempio, per le regole con un'Challengeazione CAPTCHA o, `challengeResponse` verrà elencato l'`captchaResponseo`. Se la regola corrispondente fa parte di un gruppo di regole e hai sovrascritto l'azione della regola configurata, l'azione configurata verrà fornita in. `overriddenAction`

terminatingRuleId

ID della regola che ha terminato la richiesta. Se non viene terminata la richiesta, il valore è `Default_Action`.

terminatingRuleMatchDettagli

Informazioni dettagliate sulla regola di terminazione corrispondente alla richiesta. Una regola di terminazione ha un'azione che termina il processo di ispezione di una richiesta Web. Le azioni possibili per una regola di terminazione includonoAllow, BlockCAPTCHA, eChallenge. Durante l'ispezione di una richiesta Web, alla prima regola che corrisponde alla richiesta e che prevede un'azione di terminazione, AWS WAF interrompe l'ispezione e applica l'azione. La richiesta web potrebbe contenere altre minacce, oltre a quella riportata nel registro per la regola di terminazione corrispondente.

Questo viene popolato solo per le istruzioni delle regole di corrispondenza SQL injection e Cross-site scripting (XSS). La regola di abbinamento potrebbe richiedere una corrispondenza per più di un criterio di ispezione, pertanto questi dettagli di corrispondenza vengono forniti come una serie di criteri di corrispondenza.

terminatingRuleType

Tipo della regola che ha terminato la richiesta. Valori possibili: RATE_BASED, REGULAR, GROUP e MANAGED_RULE_GROUP.

timestamp

Time Stamp in millisecondi.

uri

URI della richiesta.

webaclId

GUID dell'ACL Web.

Esempi di log

Example Regola 1 basata sulla tariffa: configurazione delle regole con una chiave, impostata su **`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 Regola basata sulla tariffa 1: immissione del registro per la richiesta bloccata dalla regola basata sulla tariffa

```
{
   "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 Regola 2 basata sulla tariffa: configurazione delle regole con due chiavi, impostata su e **`Header:dognameHeader: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 Regola basata sulla tariffa 2: immissione del registro per la richiesta bloccata dalla regola basata sulla tariffa

```
{
   "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 Output di registro per una regola attivata al momento del rilevamento SQLi (terminazione)

```
{
    "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 Output di log per una regola attivata al momento del rilevamento SQLi (non terminante)

```
{
    "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 Output di log per più regole attivate all'interno di un gruppo di regole (Rulea-XSS termina e Rule-B non termina)

```
{
    "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 Output di log per una regola attivata per l'ispezione del corpo della richiesta con tipo di contenuto JSON

AWS WAF attualmente riporta la posizione dell'ispezione del corpo JSON come. `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 Registra l'output di una regola CAPTCHA in base a una richiesta web con un token CAPTCHA valido e non scaduto

Il seguente elenco di log riguarda una richiesta Web che corrisponde a una regola con un'azione. CAPTCHA La richiesta web ha un token CAPTCHA valido e non scaduto e viene annotata solo come corrispondenza CAPTCHA da AWS WAF, in modo simile al comportamento dell'azione. Count Questa corrispondenza CAPTCHA è indicata sotto. `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 Registra l'output di una regola CAPTCHA rispetto a una richiesta web che non ha un token CAPTCHA

Il seguente elenco di log riguarda una richiesta Web che corrisponde a una regola con un'azione. CAPTCHA La richiesta web non aveva un token CAPTCHA ed è stata bloccata da. 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"
  }
}
```


Test e ottimizzazione delle protezioni AWS WAF

Ti consigliamo di testare e ottimizzare eventuali modifiche all'ACL AWS WAF Web prima di applicarle al traffico del sito Web o dell'applicazione Web.

> **⚠ Rischio legato al traffico di produzione**
>
> Prima di implementare l'implementazione Web ACL per il traffico di produzione, testala e ottimizzala in un ambiente di staging o di test finché non ti rendi conto del potenziale impatto sul traffico. Quindi testa e ottimizza le regole in modalità di conteggio con il traffico di produzione prima di abilitarle.

Questa sezione fornisce indicazioni per testare e ottimizzare gli ACL AWS WAF Web, le regole, i gruppi di regole, i set IP e i set di pattern regex.

Questa sezione fornisce anche linee guida generali per testare l'utilizzo di gruppi di regole gestiti da qualcun altro. Questi includono i gruppi di regole AWS Marketplace AWS Managed Rules, i gruppi di regole gestiti e i gruppi di regole condivisi con te da un altro account. Per questi gruppi di regole, segui anche le indicazioni fornite dal fornitore del gruppo di regole.

- Per il gruppo di regole Bot Control AWS Managed Rules, vedi anche Test e implementazione di AWS WAF Bot Control.
- Per il gruppo di regole AWS Managed Rules per la prevenzione dell'acquisizione di account, vedi Test e implementazione dell'ATP anche.
- Per il gruppo di regole AWS Managed Rules per la prevenzione delle frodi per la creazione di account, vedi Test e implementazione di ACFP anche.

Incoerenze temporanee durante gli aggiornamenti

Quando si crea o si modifica un ACL Web o altre AWS WAF risorse, le modifiche richiedono poco tempo per essere propagate in tutte le aree in cui sono archiviate le risorse. Il tempo di propagazione può variare da pochi secondi a diversi minuti.

Di seguito sono riportati alcuni esempi delle incongruenze temporanee che potreste notare durante la propagazione delle modifiche:

- Dopo aver creato un ACL Web, se si tenta di associarlo a una risorsa, è possibile che venga visualizzata un'eccezione che indica che l'ACL Web non è disponibile.
- Dopo aver aggiunto un gruppo di regole a un ACL Web, le nuove regole del gruppo di regole potrebbero essere in vigore in un'area in cui viene utilizzato l'ACL Web e non in un'altra.
- Dopo aver modificato l'impostazione di un'azione della regola, è possibile vedere la vecchia azione in alcuni punti e la nuova azione in altri.
- Dopo aver aggiunto un indirizzo IP a un set IP utilizzato in una regola di blocco, il nuovo indirizzo potrebbe essere bloccato in un'area mentre è ancora consentito in un'altra.

Test e ottimizzazione di passaggi di alto livello

Questa sezione fornisce un elenco di controllo dei passaggi per testare le modifiche all'ACL Web, comprese le regole o i gruppi di regole utilizzati.

> **Note**
>
> Per seguire le indicazioni contenute in questa sezione, devi capire come creare e gestire AWS WAF protezioni come ACL web, regole e gruppi di regole. Queste informazioni sono trattate nelle sezioni precedenti di questa guida.

Per testare e ottimizzare il tuo ACL web

Esegui questi passaggi prima in un ambiente di test, poi in produzione.

1. Preparati per il test

   Prepara il tuo ambiente di monitoraggio, imposta le nuove AWS WAF protezioni in modalità di conteggio per i test e crea tutte le associazioni di risorse di cui hai bisogno.

   Per informazioni, consulta Preparazione per i test.
2. Monitora e ottimizza gli ambienti di test e produzione

   Monitora e regola AWS WAF le protezioni prima in un ambiente di test o staging, poi in produzione, finché non sarai sicuro che siano in grado di gestire il traffico secondo le tue esigenze.

   Per informazioni, consulta Monitoraggio e ottimizzazione.
3. Attiva le tue protezioni in produzione

   Quando sei soddisfatto delle protezioni utilizzate nei test, passa alla modalità di produzione, elimina eventuali artefatti dei test non necessari e continua il monitoraggio.

   Per informazioni, consulta Attivazione delle protezioni in produzione.

Dopo aver completato l'implementazione delle modifiche, continua a monitorare il traffico web e le protezioni in produzione per assicurarti che funzionino come desideri. I modelli di traffico web possono cambiare nel tempo, quindi potresti dover modificare le protezioni di tanto in tanto.

Preparazione per i test

Questa sezione descrive come prepararti per testare e ottimizzare le tue AWS WAF protezioni.

> **Note**
>
> Per seguire le indicazioni contenute in questa sezione, è necessario comprendere in generale come creare e gestire AWS WAF protezioni come ACL Web, regole e gruppi di regole. Queste informazioni sono trattate nelle sezioni precedenti di questa guida.

Per prepararsi al test

1. Abilita la registrazione ACL Web, le CloudWatch metriche Amazon e il campionamento delle richieste Web per l'ACL Web

   Utilizza la registrazione, le metriche e il campionamento per monitorare l'interazione delle regole Web ACL con il tuo traffico web.

   - Registrazione: è possibile configurare la registrazione delle richieste Web valutate AWS WAF da un ACL Web. Puoi inviare i log ai CloudWatch log, a un bucket Amazon S3 o a un Amazon Data Firehose. Puoi oscurare i campi e applicare filtri. Per ulteriori informazioni, consulta Registrazione del traffico AWS WAF ACL Web.
   - CloudWatch Parametri Amazon: nella configurazione Web ACL, fornisci le specifiche dei parametri per tutto ciò che desideri monitorare. Puoi visualizzare le metriche tramite le console e. AWS WAF CloudWatch Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch.
   - Campionamento delle richieste Web: puoi visualizzare un esempio di tutte le richieste Web valutate dall'ACL Web. Per informazioni sul campionamento delle richieste Web, vedere. Visualizzazione di un esempio di richieste Web
2. Imposta le tue protezioni sulla modalità Count

   Nella configurazione Web ACL, passa alla modalità di conteggio tutto ciò che desideri testare. Ciò fa sì che le protezioni di test registrino le corrispondenze con le richieste Web senza alterare il modo in cui le richieste vengono gestite. Potrai vedere le corrispondenze nelle tue metriche, nei log e nelle richieste campionate, verificare i criteri di corrispondenza e capire quali potrebbero essere gli effetti sul tuo traffico web. Le regole che aggiungono etichette alle richieste corrispondenti aggiungeranno etichette indipendentemente dall'azione della regola.

   - Regola definita nell'ACL Web: modifica le regole nell'ACL Web e imposta le relative azioni su. Count

- Gruppo di regole: nella configurazione dell'ACL Web, modifica l'istruzione della regola per il gruppo di regole e, nel riquadro Regole, apri il menu a discesa Sostituisci tutte le azioni delle regole e scegli. Count Se gestisci l'ACL web in JSON, aggiungi le regole alle `RuleActionOverrides` impostazioni nell'istruzione di riferimento del gruppo di regole, con set to. `ActionToUse` Count L'elenco di esempio seguente mostra le sostituzioni per due regole nel gruppo di regole `AWSManagedRulesAnonymousIpList` AWS Managed Rules.

```
"ManagedRuleGroupStatement": {
  "VendorName": "AWS",
  "Name": "AWSManagedRulesAnonymousIpList",
    "RuleActionOverrides": [
      {
        "ActionToUse": {
          "Count": {}
        },
        "Name": "AnonymousIPList"
      },
      {
        "ActionToUse": {
          "Count": {}
        },
        "Name": "HostingProviderIPList"
      }
    ],
    "ExcludedRules": []
  }
},
```

  Per ulteriori informazioni sulle sostituzioni delle azioni delle regole, consulta. Sovrascrivere le azioni delle regole in un gruppo di regole

  Per il tuo gruppo di regole, non modificare le azioni delle regole nel gruppo di regole stesso. Le regole dei gruppi di regole con Count azione non generano le metriche o gli altri artefatti necessari per i test. Inoltre, la modifica di un gruppo di regole influisce su tutti gli ACL Web che lo utilizzano, mentre le modifiche all'interno della configurazione ACL Web influiscono solo sul singolo ACL Web.

- Web ACL: se stai testando un nuovo ACL Web, imposta l'azione predefinita per l'ACL Web per consentire le richieste. In questo modo puoi provare l'ACL web senza influire in alcun modo sul traffico.

In generale, la modalità di conteggio genera più corrispondenze rispetto alla produzione. Questo perché una regola che conta le richieste non interrompe la valutazione della richiesta da parte dell'ACL Web, pertanto anche le regole che verranno eseguite successivamente nell'ACL Web potrebbero corrispondere alla richiesta. Quando modifichi le azioni delle regole impostandone le impostazioni di produzione, le regole che consentono o bloccano le richieste interromperanno la valutazione delle richieste corrispondenti. Di conseguenza, le richieste corrispondenti verranno generalmente esaminate in base a un minor numero di regole nell'ACL Web. Per ulteriori informazioni sugli effetti delle azioni delle regole sulla valutazione complessiva di una richiesta Web, vedere. Operazione delle regole

Con queste impostazioni, le nuove protezioni non altereranno il traffico web, ma genereranno informazioni sulle corrispondenze nelle metriche, nei log ACL Web e negli esempi di richieste.

3. Associa l'ACL Web a una risorsa

   Se l'ACL Web non è già associato alla risorsa, associalo.

   Per informazioni, consulta Associazione o dissociazione di un ACL Web con una risorsa AWS.

Ora sei pronto per monitorare e ottimizzare il tuo ACL web.

Monitoraggio e ottimizzazione

Questa sezione descrive come monitorare e ottimizzare le AWS WAF protezioni.

> **Note**
>
> Per seguire le indicazioni contenute in questa sezione, è necessario comprendere in generale come creare e gestire AWS WAF protezioni come ACL Web, regole e gruppi di regole. Queste informazioni sono trattate nelle sezioni precedenti di questa guida.

Monitora il traffico web e la corrispondenza delle regole per verificare il comportamento dell'ACL web. Se riscontri problemi, modifica le regole per correggerle, quindi monitora per verificare le modifiche.

Ripeti la procedura seguente finché l'ACL Web non gestirà il traffico Web come richiesto.

Per monitorare e ottimizzare

1. Monitora il traffico e regola le corrispondenze

   Assicurati che il traffico scorra e che le regole del test trovino le richieste corrispondenti.

   Cerca le seguenti informazioni per le protezioni che stai testando:

   - Registri: accedi alle informazioni sulle regole che corrispondono a una richiesta web:
     - Le tue regole: le regole dell'ACL Web che prevedono Count un'azione sono elencate di seguito. `nonTerminatingMatchingRules` Le regole con Allow o Block sono elencate come. `terminatingRule` Le regole con CAPTCHA o Challenge possono essere terminanti o non terminanti, e quindi sono elencate in una delle due categorie, in base al risultato della corrispondenza delle regole.
     - Gruppi di regole: i gruppi di regole sono identificati nel `ruleGroupId` campo e le rispettive corrispondenze di regole sono classificate nella stessa categoria delle regole autonome.
     - Etichette: le etichette che le regole hanno applicato alla richiesta sono elencate nel `Labels` campo.

     Per ulteriori informazioni, consulta Campi di log.
   - CloudWatch Parametri Amazon: puoi accedere ai seguenti parametri per la valutazione della tua richiesta ACL Web.
     - Le tue regole: le metriche sono raggruppate in base all'azione della regola. Ad esempio, quando si verifica una regola in Count modalità, le relative corrispondenze vengono elencate come `Count` metriche per l'ACL Web.
     - I tuoi gruppi di regole: le metriche per i tuoi gruppi di regole sono elencate sotto le metriche dei gruppi di regole.
     - Gruppi di regole di proprietà di un altro account: le metriche dei gruppi di regole sono generalmente visibili solo al proprietario del gruppo di regole. Tuttavia, se sovrascrivi l'azione della regola per una regola, le metriche relative a tale regola verranno elencate nelle metriche ACL Web. Inoltre, le etichette aggiunte da qualsiasi gruppo di regole sono elencate nelle metriche ACL Web

       I gruppi di regole di questa categoria sonoAWS Regole gestite per AWS WAF, Marketplace AWS gruppi di regole gestitiGruppi di regole forniti da altri servizi, e i gruppi di regole condivisi con te da un altro account.

- Etichette: le etichette che sono state aggiunte a una richiesta Web durante la valutazione sono elencate nelle metriche delle etichette Web ACL. Puoi accedere alle metriche per tutte le etichette, indipendentemente dal fatto che siano state aggiunte dalle tue regole e dai tuoi gruppi di regole o dalle regole di un gruppo di regole di proprietà di un altro account.

Per ulteriori informazioni, consulta Visualizzazione delle metriche per il tuo ACL web.

- Dashboard di panoramica sul traffico ACL Web: accedi ai riepiloghi del traffico Web valutato da un ACL Web accedendo alla pagina dell'ACL Web nella AWS WAF console e aprendo la scheda Panoramica del traffico.

  Le dashboard di panoramica del traffico forniscono riepiloghi quasi in tempo reale delle CloudWatch metriche di Amazon AWS WAF raccolte durante la valutazione del traffico web dell'applicazione.

  Per ulteriori informazioni, consulta Dashboard di panoramica sul traffico ACL Web.

- Richieste Web campionate: accedi alle informazioni relative alle regole che corrispondono a un campione di richieste Web. Le informazioni di esempio identificano le regole di corrispondenza in base al nome della metrica della regola nell'ACL Web. Per i gruppi di regole, la metrica identifica la dichiarazione di riferimento del gruppo di regole. Per le regole all'interno dei gruppi di regole, l'esempio elenca il nome della regola corrispondente in. `RuleWithinRuleGroup`

  Per ulteriori informazioni, consulta Visualizzazione di un esempio di richieste Web.

2. Configura le mitigazioni per risolvere i falsi positivi

   Se stabilisci che una regola genera falsi positivi, abbinando le richieste Web laddove non dovrebbe, le seguenti opzioni possono aiutarti a ottimizzare le protezioni ACL Web per mitigare la situazione.

   Correzione dei criteri di ispezione delle regole

   Per quanto riguarda le regole, spesso è sufficiente modificare le impostazioni che si utilizzano per esaminare le richieste Web. Gli esempi includono la modifica delle specifiche in un set di pattern regex, la regolazione delle trasformazioni di testo applicate a un componente della richiesta prima dell'ispezione o il passaggio all'utilizzo di un indirizzo IP inoltrato. Consulta la guida per il tipo di regola che causa problemi, sotto. Nozioni di base sulla dichiarazione delle regole

   Correzione di problemi più complessi

Per i criteri di ispezione che non controllate e per alcune regole complesse, potrebbe essere necessario apportare altre modifiche, ad esempio aggiungere regole che consentano o blocchino esplicitamente le richieste o che eliminino le richieste dalla valutazione in base alla regola problematica. I gruppi di regole gestiti richiedono in genere questo tipo di mitigazione, ma lo possono fare anche altre regole. Gli esempi includono l'istruzione Rate-Based Rule e l'istruzione SQL Injection Attack Rule.

Ciò che fai per mitigare i falsi positivi dipende dal tuo caso d'uso. Gli approcci più comuni sono i seguenti:

- Aggiungi una regola di attenuazione: aggiungi una regola che viene eseguita prima della nuova regola e che consente esplicitamente le richieste che causano falsi positivi. Per informazioni sull'ordine di valutazione delle regole in un ACL Web, vedere. Ordine di elaborazione delle regole e dei gruppi di regole in un ACL Web

  Con questo approccio, le richieste consentite vengono inviate alla risorsa protetta, in modo che non raggiungano mai la nuova regola di valutazione. Se la nuova regola è un gruppo di regole gestito a pagamento, questo approccio può anche aiutare a contenere i costi legati all'utilizzo del gruppo di regole.
- Aggiungi una regola logica con una regola attenuante: utilizza le istruzioni delle regole logiche per combinare la nuova regola con una regola che esclude i falsi positivi. Per informazioni, consulta Dichiarazioni di regole logiche.

  Ad esempio, supponiamo che tu stia aggiungendo un'istruzione SQL injection attack match che genera falsi positivi per una categoria di richieste. Create una regola che corrisponda a tali richieste, quindi combinate le regole utilizzando istruzioni di regole logiche in modo da ottenere la corrispondenza solo per le richieste che non soddisfano i criteri dei falsi positivi e soddisfano i criteri di attacco SQL injection.
- Aggiungi un'istruzione scope-down: per le istruzioni basate sulla frequenza e le istruzioni di riferimento per gruppi di regole gestite, escludi dalla valutazione le richieste che generano falsi positivi aggiungendo un'istruzione scope-down all'interno dell'istruzione principale.

  Una richiesta che non corrisponde all'istruzione scope-down non raggiunge mai il gruppo di regole o la valutazione basata sulla frequenza. Per informazioni sulle istruzioni scope-down, consulta. Dichiarazioni delimitate Per vedere un esempio, consulta Escludi l'intervallo IP dalla gestione dei bot.

- Aggiungi una regola di corrispondenza delle etichette: per i gruppi di regole che utilizzano l'etichettatura, identifica l'etichetta che la regola problematica sta applicando alle richieste. Potrebbe essere necessario impostare prima le regole del gruppo di regole in modalità conteggio, se non l'hai già fatto. Aggiungi una regola di corrispondenza delle etichette, posizionata in modo da seguire il gruppo di regole, che corrisponda all'etichetta aggiunta dalla regola problematica. Nella regola di corrispondenza delle etichette, puoi filtrare le richieste che desideri consentire da quelle che desideri bloccare.

  Se utilizzi questo approccio, al termine del test, mantieni la regola problematica in modalità di conteggio nel gruppo di regole e mantieni valida la regola di abbinamento delle etichette personalizzata. Per informazioni sulle istruzioni di abbinamento delle etichette, consultaDichiarazione della regola di corrispondenza delle etichette. Per alcuni esempi, consulta Consenti uno specifico bot bloccato e Esempio ATP: gestione personalizzata delle credenziali mancanti e compromesse.
- Modifica della versione di un gruppo di regole gestito: per i gruppi di regole gestiti con versioni diverse, modifica la versione che stai utilizzando. Ad esempio, puoi tornare all'ultima versione statica che stavi utilizzando correttamente.

  Di solito si tratta di una soluzione temporanea. È possibile modificare la versione per il traffico di produzione mentre si continua a testare la versione più recente nell'ambiente di test o di staging o mentre si attende una versione più compatibile fornita dal provider. Per informazioni sulle versioni dei gruppi di regole gestiti, consultaGruppi di regole gestite.

Quando ritieni che le nuove regole soddisfino le richieste necessarie, passa alla fase successiva del test e ripeti questa procedura. Eseguite la fase finale di test e ottimizzazione nel vostro ambiente di produzione.

Visualizzazione delle metriche per il tuo ACL web

Dopo aver associato un ACL Web a una o più AWS risorse, puoi visualizzare le metriche risultanti per l'associazione in un grafico Amazon CloudWatch .

Per informazioni sulle AWS WAF metriche, consulta. AWS WAF metriche e dimensioni Per informazioni sui CloudWatch parametri, consulta la Amazon CloudWatch User Guide.

Per ciascuna delle tue regole in un ACL web e per tutte le richieste a cui una risorsa associata inoltra AWS WAF per un ACL web, ti CloudWatch consente di fare quanto segue:

- Visualizza i dati dell'ora precedente o delle tre ore precedenti.
- Modifica l'intervallo tra i punti dati.
- Modifica il calcolo che CloudWatch viene eseguito sui dati, ad esempio massimo, minimo, media o somma.

> **Note**
>
> AWS WAF with CloudFront è un servizio globale e le metriche sono disponibili solo quando scegli la regione Stati Uniti orientali (Virginia settentrionale) nella. AWS Management Console Se scegli un'altra regione, non verrà visualizzata alcuna AWS WAF metrica nella console. CloudWatch

Per visualizzare i dati per le regole di un'ACL Web

1. Accedi AWS Management Console e apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Se necessario, cambia la regione con quella in cui si trovano le AWS risorse. Per CloudFront, scegli la regione Stati Uniti orientali (Virginia settentrionale).
3. Nel riquadro di navigazione, in Metriche, scegli Tutte le metriche, quindi cerca nella scheda Sfoglia. `AWS::WAFV2`
4. Selezionare la casella di controllo per l'ACL Web da aggiornare.
5. Modificare le impostazioni applicabili:

   Statistic

   Scegli il calcolo che viene CloudWatch eseguito sui dati.

   Intervallo temporale

   Scegliere se visualizzare i dati per l'ora precedente o le tre ore precedenti.

   Periodo

   Scegliere l'intervallo tra punti dati nel grafico.

   Regolamento

   Scegliere le regole per cui visualizzare i dati.

> **Note**
>
> Se modifichi il nome di una regola e desideri che il nome della metrica della regola rifletta la modifica, devi aggiornare anche il nome della metrica. AWS WAF non aggiorna automaticamente il nome della metrica di una regola quando si modifica il nome della regola. Puoi cambiare il nome della metrica quando modifichi la regola nella console, utilizzando l'editor JSON delle regole. Puoi anche modificare entrambi i nomi tramite le API e in qualsiasi elenco JSON che utilizzi per definire l'ACL web o il gruppo di regole.

Tieni presente quanto segue:

- Se di recente hai associato un ACL Web a una AWS risorsa, potresti dover attendere alcuni minuti prima che i dati vengano visualizzati nel grafico e che la metrica per l'ACL Web compaia nell'elenco delle metriche disponibili.
- Se associ più di una risorsa a un ACL web, CloudWatch i dati includeranno le richieste per tutte.
- È possibile posizionare il cursore su un punto dati per ottenere ulteriori informazioni.
- Il grafico non si aggiorna automaticamente. Per aggiornare la visualizzazione, scegliere l'icona di aggiornamento
  ().

Per ulteriori informazioni sulle CloudWatch metriche, consulta. Monitoraggio con Amazon CloudWatch

Dashboard di panoramica sul traffico ACL Web

Questa sezione descrive i dashboard di panoramica del traffico ACL Web disponibili nella console. AWS WAF Dopo aver associato un ACL Web a una o più AWS risorse e abilitato le metriche per l'ACL Web, puoi accedere ai riepiloghi del traffico Web valutato dall'ACL Web accedendo alla scheda Panoramica del traffico dell'ACL Web nella console. AWS WAF Le dashboard includono riepiloghi quasi in tempo reale delle CloudWatch metriche di Amazon AWS WAF raccolte durante la valutazione del traffico web dell'applicazione.

> **Note**
>
> Se non vedi nulla nei dashboard, assicurati di avere le metriche abilitate per l'ACL web.

La scheda Panoramica del traffico di Web ACL contiene dashboard a schede con le seguenti categorie di informazioni:

- Tutto il traffico: tutte le richieste Web valutate dall'ACL Web.

  La dashboard si concentra sull'interruzione delle azioni, ma puoi visualizzare le corrispondenze per le regole di conteggio nelle seguenti posizioni:

  - Pannello delle 10 regole principali di questa dashboard. Attiva Passa al conteggio delle azioni per mostrare le corrispondenze alle regole del conteggio.
  - Scheda delle richieste esemplificate della pagina Web ACL. Questa nuova scheda include un grafico di tutte le corrispondenze delle regole. Per informazioni, consulta Visualizzazione di un esempio di richieste Web.
- Bot Control: richieste Web che l'ACL Web valuta utilizzando il gruppo di regole gestito da Bot Control.

  Se non utilizzi questo gruppo di regole nell'ACL web, questa scheda mostra i risultati della valutazione di un campione del tuo traffico web rispetto alle regole di Bot Control. Questo ti dà un'idea del traffico bot che riceve la tua applicazione ed è gratuito.

  Questo gruppo di regole fa parte delle opzioni intelligenti di mitigazione delle minacce AWS WAF offerte. Per ulteriori informazioni, consultare AWS WAF Controllo dei bot e AWS WAF Gruppo di regole Bot Control.
- Prevenzione dell'acquisizione di account: richieste Web che l'ACL Web valuta utilizzando il gruppo di regole gestito per la prevenzione dell'acquisizione degli account (ATP) di AWS WAF Fraud Control. Questa scheda è disponibile solo se utilizzi questo gruppo di regole nell'ACL web.

  Il gruppo di regole ATP fa parte delle offerte di mitigazione AWS WAF intelligente delle minacce. Per ulteriori informazioni, consultare AWS WAF Controllo delle frodi e prevenzione delle acquisizioni di conti (ATP) e AWS WAF Gruppo di regole per la prevenzione delle acquisizioni di account (ATP) per il controllo delle frodi.
- Prevenzione delle frodi nella creazione di account: richieste Web che l'ACL Web valuta utilizzando il gruppo di regole gestito per la prevenzione delle AWS WAF frodi per la creazione di account

Fraud Control (ACFP). Questa scheda è disponibile solo se utilizzi questo gruppo di regole nell'ACL web.

Il gruppo di regole ACFP fa parte delle offerte di mitigazione AWS WAF intelligente delle minacce. Per ulteriori informazioni, consultare AWS WAF Fraud Control creazione di account e prevenzione delle frodi (ACFP) e AWS WAF Gruppo di regole per la prevenzione delle frodi (ACFP) per la creazione di account Fraud Control.

I dashboard si basano sulle metriche dell'ACL Web e i grafici forniscono l'accesso alle CloudWatch metriche corrispondenti in. CloudWatch Per le dashboard intelligenti di mitigazione delle minacce, come Bot Control, le metriche utilizzate sono principalmente le metriche delle etichette.

- Per un elenco delle metriche fornite, consulta. AWS WAF AWS WAF metriche e dimensioni
- Per informazioni sui CloudWatch parametri, consulta la Amazon CloudWatch User Guide.

Le dashboard forniscono riepiloghi dei modelli di traffico per le azioni terminali e l'intervallo di date selezionato. Le dashboard di mitigazione intelligente delle minacce includono le richieste valutate dal corrispondente gruppo di regole gestite, indipendentemente dal fatto che sia stato lo stesso gruppo di regole gestite ad applicare l'azione di cessazione. Ad esempio, se Block è selezionata, la dashboard di prevenzione dell'acquisizione di account include informazioni per tutte le richieste Web che sono state entrambe valutate dal gruppo di regole gestite dall'ATP e bloccate a un certo punto durante la valutazione dell'ACL Web. Le richieste possono essere bloccate dal gruppo di regole gestito da ATP, da una regola eseguita dopo il gruppo di regole nell'ACL Web o dall'azione predefinita dell'ACL Web.

Visualizzazione dei dashboard per un ACL Web

Segui la procedura in questa sezione per accedere ai dashboard ACL Web e impostare i criteri di filtraggio dei dati. Se di recente hai associato un ACL Web a una AWS risorsa, potresti dover attendere alcuni minuti prima che i dati diventino disponibili nei dashboard.

I dashboard includono le richieste per tutte le risorse che hai associato all'ACL web.

Per visualizzare le dashboard di panoramica sul traffico per un ACL web

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, scegli ACL Web, quindi cerca l'ACL Web che ti interessa.

3. Seleziona l'ACL web. La console ti porta alla pagina Web dell'ACL. La scheda Panoramica del traffico è selezionata per impostazione predefinita.
4. Modifica le impostazioni dei filtri dati in base alle esigenze.

   - Interruzione delle azioni relative alle regole: seleziona le azioni di terminazione da includere nei dashboard. I dashboard riepilogano le metriche per le richieste Web a cui è stata applicata una delle azioni selezionate dalla valutazione dell'ACL Web. Se si selezionano tutte le azioni disponibili, le dashboard includono tutte le richieste Web valutate. Per informazioni sulle azioni, consulta. Come vengono gestite le azioni delle regole e dei gruppi di regole in un ACL Web
   - Intervallo di tempo: seleziona l'intervallo di tempo da visualizzare nei dashboard. Puoi scegliere di visualizzare un intervallo di tempo relativo a quello attuale, ad esempio le ultime 3 ore o l'ultima settimana, e puoi selezionare un intervallo di tempo assoluto da un calendario.
   - Fuso orario: questa impostazione si applica quando si specifica un intervallo di tempo assoluto. È possibile utilizzare il fuso orario locale del browser o l'UTC (Coordinated Universal Time).

Controlla le informazioni nelle schede che ti interessano. Le selezioni del filtro dei dati si applicano a tutte le dashboard. Nei riquadri del grafico, puoi posizionare il cursore su un punto dati o un'area per visualizzare eventuali dettagli aggiuntivi.

Countregole d'azione

È possibile visualizzare le informazioni relative al conteggio delle partite in corso in uno dei due punti seguenti.

- In questa scheda Panoramica del traffico, nella dashboard Tutto il traffico, trova il riquadro delle 10 regole principali e attiva Passa per contare le azioni. Con questa opzione attiva, il riquadro mostra le corrispondenze delle regole di conteggio invece di terminare le corrispondenze alle regole.
- Nella scheda Richieste campionate del Web ACL, visualizza un grafico di tutte le corrispondenze e le azioni delle regole per l'intervallo di tempo che hai impostato nella scheda Panoramica del traffico. Per informazioni sulla scheda Richieste campionate, consulta. Visualizzazione di un esempio di richieste Web

CloudWatch Metriche Amazon

Nei riquadri grafici della dashboard, puoi accedere alle CloudWatch metriche per i dati rappresentati graficamente. Scegli l'opzione nella parte superiore del riquadro grafico o dal menu a discesa ⋮ (ellissi verticali) all'interno del riquadro.

Aggiornamento dei dashboard

I dashboard non si aggiornano automaticamente. Per aggiornare lo schermo, scegli l'icona di aggiornamento

Esempi di dashboard di panoramica del traffico per gli ACL Web

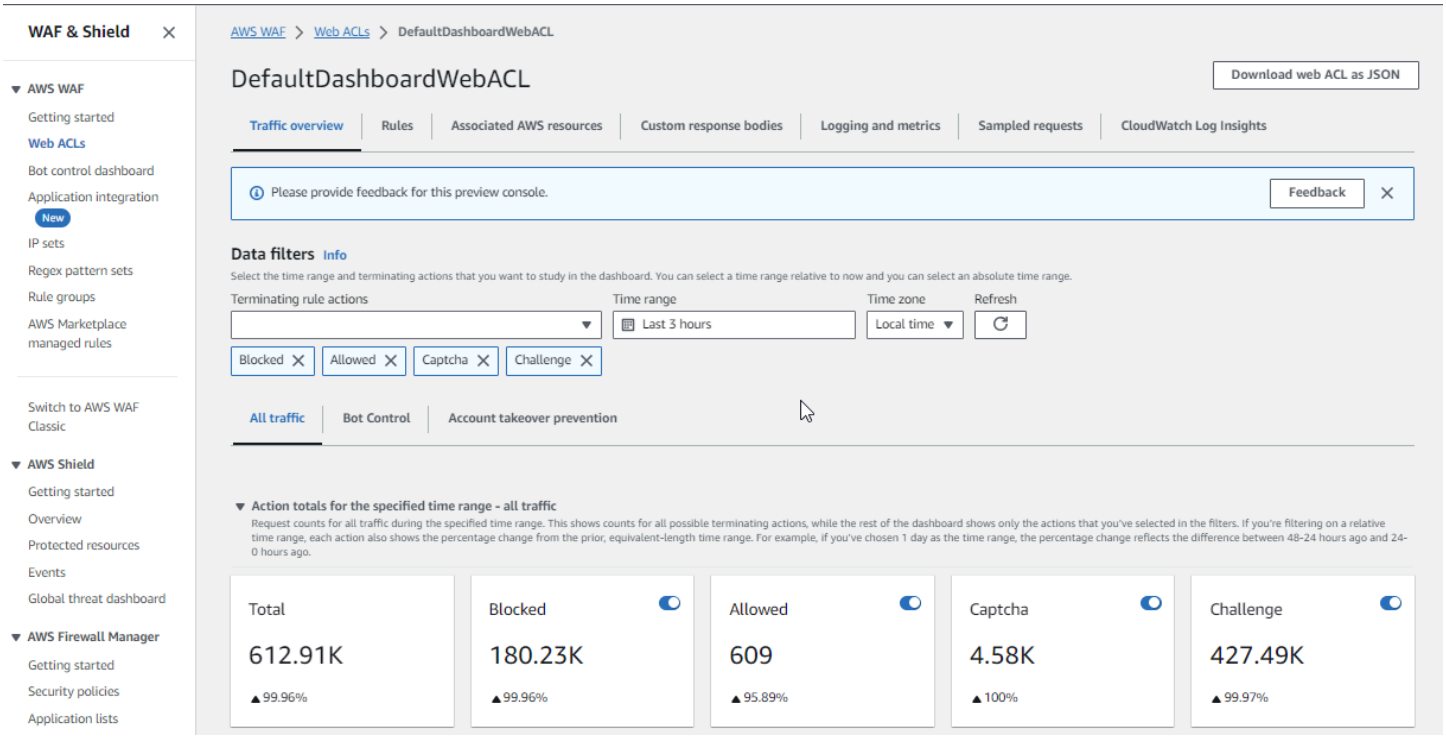
Questa sezione mostra schermate di esempio delle dashboard di panoramica del traffico per gli ACL web.

> **Note**
>
> Se lo utilizzi già AWS WAF per proteggere le risorse delle tue applicazioni, puoi visualizzare i dashboard di tutti gli ACL Web nella relativa pagina nella console. AWS WAF Per informazioni, consulta Visualizzazione dei dashboard per un ACL Web.

Schermata di esempio: i filtri dei dati e il conteggio delle azioni del dashboard All Traffic

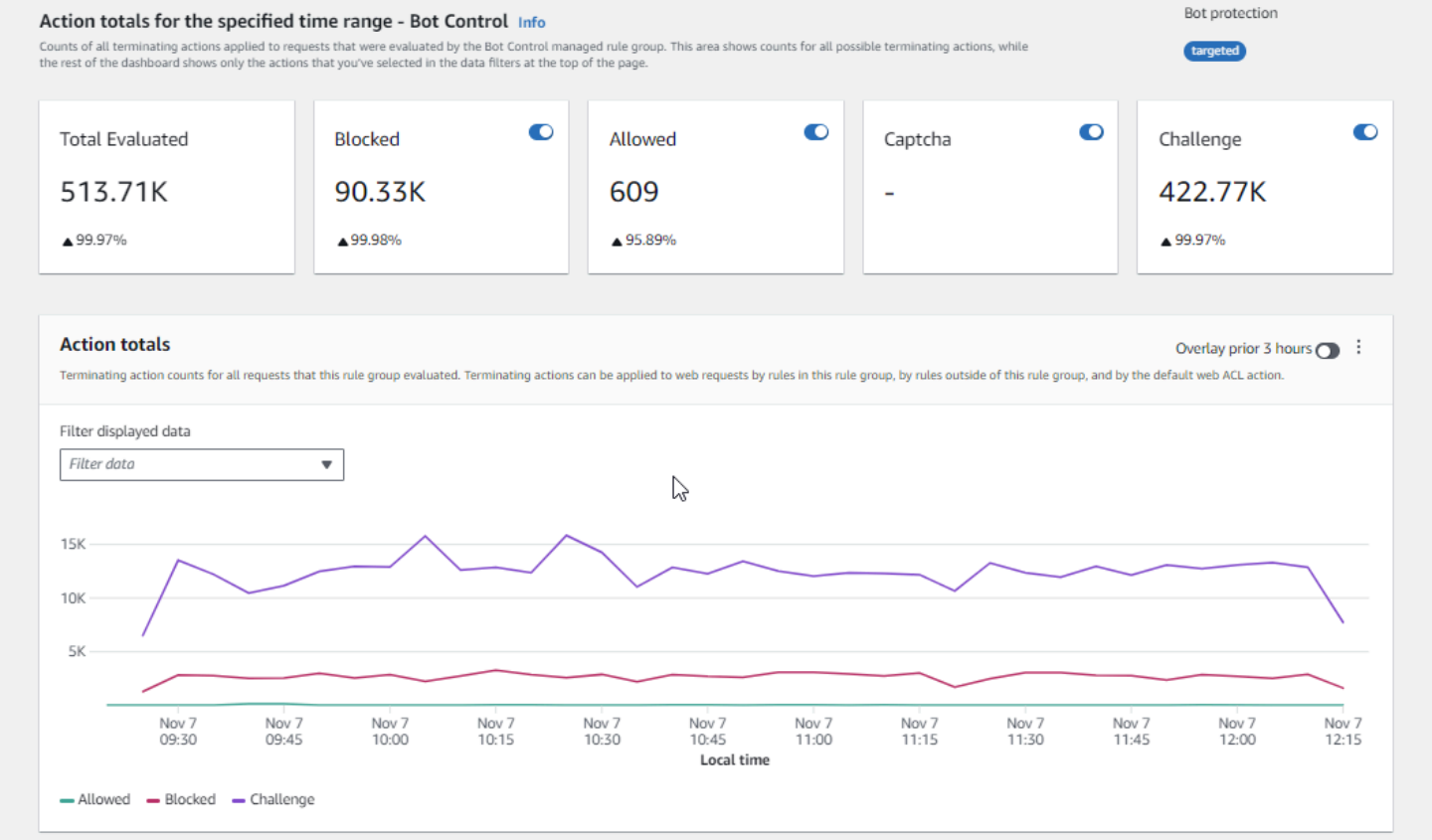
La schermata seguente mostra la panoramica del traffico per un ACL web con la scheda Tutto il traffico selezionata. I filtri di dati sono impostati sui valori predefiniti: tutte le azioni terminali delle ultime tre ore.

All'interno della dashboard dedicata a tutto il traffico sono presenti i totali delle azioni per le varie azioni terminali. Ogni riquadro elenca il numero di richieste e mostra una freccia su/giù che indica la modifica rispetto all'intervallo di tempo delle tre ore precedenti.



Schermata di esempio: conteggi delle azioni della dashboard di Bot Control

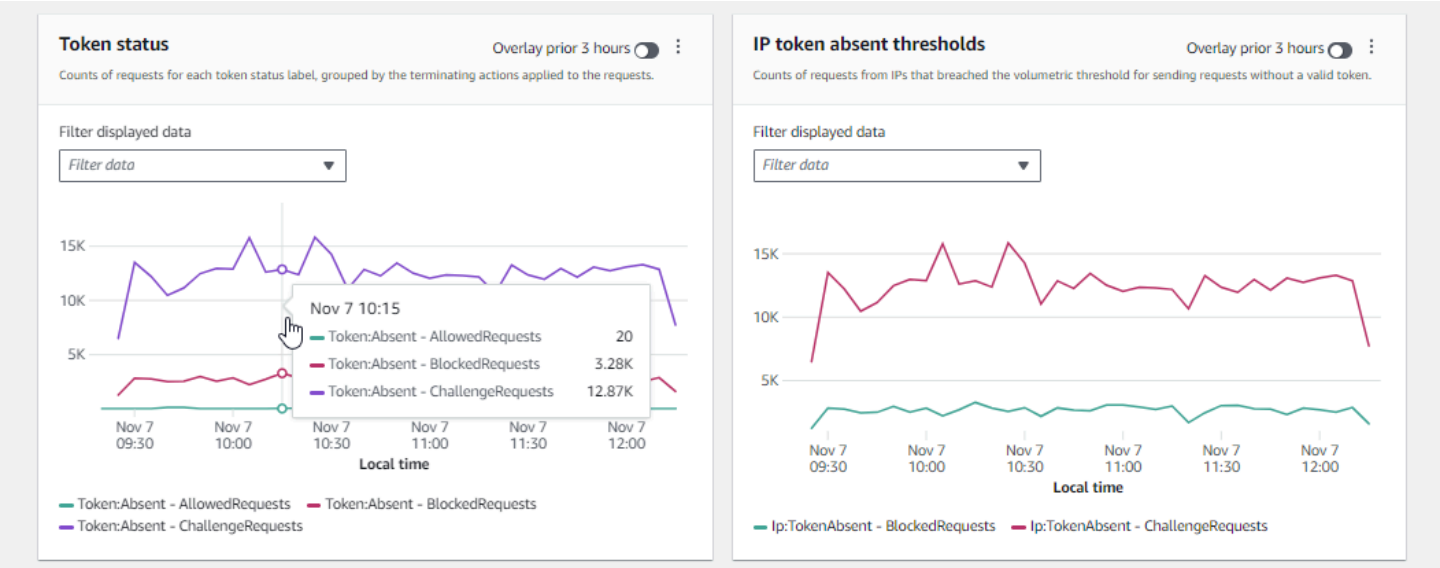
La schermata seguente mostra il conteggio delle azioni per la dashboard di Bot Control. Questo mostra gli stessi riquadri dei totali per l'intervallo di tempo, ma i conteggi riguardano solo le richieste valutate dal gruppo di regole Bot Control. Più in basso, nel riquadro Totali delle azioni, puoi vedere il conteggio delle azioni nell'intervallo di tempo specificato di tre ore. Per questo intervallo di tempo, l'CAPTCHAazione non è stata applicata a nessuna delle richieste valutate dal gruppo di regole.



Schermata di esempio: grafici di riepilogo dello stato dei token della dashboard di Bot Control

La schermata seguente mostra due dei grafici di riepilogo disponibili nella dashboard di Bot Control. Il riquadro di stato del token mostra i conteggi per le varie etichette di stato del token, abbinati all'azione della regola applicata alla richiesta. Il riquadro delle soglie di assenza del token IP mostra i dati relativi alle richieste provenienti da IP che inviavano troppe richieste senza un token.

Passando il mouse su qualsiasi area del grafico vengono visualizzati i dettagli delle informazioni disponibili. Nel riquadro di stato del token di questa schermata, il mouse passa con il mouse su un punto nel tempo, senza trovarsi su alcuna linea del grafico, quindi la console visualizza i dati per tutte le linee in quel momento.



Questa sezione mostra solo alcuni dei riepiloghi sul traffico forniti nelle dashboard di panoramica del traffico ACL Web. Per visualizzare i dashboard di qualsiasi ACL Web, apri la pagina dell'ACL Web nella console. Per informazioni su come eseguire questa operazione, consulta la guida all'indirizzo. Visualizzazione dei dashboard per un ACL Web

Visualizzazione di un esempio di richieste Web

Questa sezione descrive la scheda Web ACL Sampled request nella console. AWS WAF In questa scheda è possibile visualizzare un grafico di tutte le corrispondenze delle regole per le richieste Web esaminate AWS WAF . Inoltre, se hai abilitato il campionamento delle richieste, puoi visualizzare una tabella di un esempio di richieste Web esaminate AWS WAF .

L'esempio di richieste contiene fino a 100 richieste che corrispondono ai criteri di una regola nell'ACL Web e altre 100 richieste di richieste che non soddisfano alcuna regola e a cui è stata applicata l'azione predefinita dell'ACL Web. Le richieste nell'esempio provengono da tutte le risorse protette che hanno ricevuto richieste per i tuoi contenuti nelle tre ore precedenti.

Quando una richiesta Web soddisfa i criteri di una regola e l'azione relativa a tale regola non interrompe la valutazione della richiesta, AWS WAF continua a esaminare la richiesta Web utilizzando le regole successive nell'ACL Web. Per questo motivo, una richiesta Web potrebbe apparire più volte. Per informazioni sui comportamenti di azione delle regole, vedereOperazione delle regole.

Per visualizzare il grafico di tutte le regole e le richieste campionate

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).
3. Scegli il nome dell'ACL web per il quale desideri visualizzare le richieste. La console consente di accedere alla descrizione dell'ACL Web, dove è possibile modificarla.
4. Nella scheda Richieste campionate, puoi vedere quanto segue:

   - Grafico di tutte le regole: questo grafico mostra le regole di corrispondenza e le azioni delle regole per tutte le valutazioni delle richieste Web eseguite durante l'intervallo di tempo indicato.

     > **Note**
     >
     > L'intervallo di tempo per questo grafico è impostato nella scheda Panoramica del traffico del Web ACL, nella sezione Filtri dati. Per informazioni, consulta Visualizzazione dei dashboard per un ACL Web.

   - Tabella delle richieste campionate: questa tabella mostra i dati campionati delle richieste delle ultime 3 ore. Per ogni voce, la tabella mostra i seguenti dati:

     Nome parametro

     Il nome della CloudWatch metrica per la regola nell'ACL Web che corrisponde alla richiesta. Se una richiesta Web non corrisponde a nessuna regola nell'ACL Web, questo valore è Predefinito.

     > **Note**
     >
     > Se modifichi il nome di una regola e desideri che il nome della metrica della regola rifletta la modifica, devi aggiornare anche il nome della metrica. AWS WAF non aggiorna automaticamente il nome della metrica di una regola quando si modifica il nome della regola. Puoi cambiare il nome della metrica quando modifichi la regola nella console, utilizzando l'editor JSON delle regole. Puoi anche modificare entrambi i nomi tramite le API e in qualsiasi elenco JSON che utilizzi per definire l'ACL web o il gruppo di regole.

IP di origine

L'indirizzo IP da cui proviene la richiesta oppure, se il visualizzatore ha utilizzato un proxy HTTP o un Application Load Balancer per inviare la richiesta, l'indirizzo IP del proxy o dell'Application Load Balancer.

URI

La parte di un URL che identifica una risorsa, ad esempio, `/images/daily-ad.jpg`.

Regola all'interno del gruppo di regole

Se il nome della metrica identifica un'istruzione di riferimento del gruppo di regole, identifica la regola all'interno del gruppo di regole che corrisponde alla richiesta.

Azione

Indica l'azione per la regola corrispondente. Per informazioni sulle possibili azioni delle regole, vedereOperazione delle regole.

Orario

L'ora in cui AWS WAF ha ricevuto la richiesta dalla risorsa protetta.

Per visualizzare informazioni aggiuntive sui componenti di una richiesta Web, scegli il nome dell'URI nella riga della richiesta.

Attivazione delle protezioni in produzione

Una volta completata la fase finale di test e ottimizzazione nell'ambiente di produzione, abilita le protezioni in modalità produzione.

> **Rischio legato al traffico di produzione**
>
> Prima di implementare l'implementazione Web ACL per il traffico di produzione, testala e ottimizzala in un ambiente di test finché non ti senti a tuo agio con il potenziale impatto sul traffico. Inoltre, testala e ottimizzala in modalità di conteggio con il traffico di produzione prima di abilitare le protezioni per il traffico di produzione.

> **Note**
>
> Per seguire le indicazioni contenute in questa sezione, è necessario comprendere in generale come creare e gestire AWS WAF protezioni come ACL Web, regole e gruppi di regole. Queste informazioni sono trattate nelle sezioni precedenti di questa guida.

Esegui questi passaggi prima nell'ambiente di test, poi in produzione.

Attiva le tue AWS WAF protezioni in produzione

1. Passa alle tue protezioni di produzione

   Aggiorna il tuo ACL web e cambia le impostazioni per la produzione.

   a. Rimuovi tutte le regole di test che non ti servono

      Se hai aggiunto regole di test che non ti servono in produzione, rimuovile. Se utilizzi delle regole di abbinamento delle etichette per filtrare i risultati delle regole gestite dei gruppi di regole, assicurati di lasciarle invariate.

   b. Passa alle azioni di produzione

      Modifica le impostazioni di azione per le nuove regole in base alle impostazioni di produzione previste.

      - Regola definita nell'ACL Web: modifica le regole nell'ACL Web e modifica le relative azioni da azioni Count di produzione.
      - Gruppo di regole: nella configurazione Web ACL del gruppo di regole, modificate le regole per utilizzare le proprie azioni o lasciate che l'Countazione venga sostituita, in base ai risultati delle attività di test e ottimizzazione. Se utilizzi una regola di abbinamento delle etichette per filtrare i risultati di una regola del gruppo di regole, assicurati di lasciare invariata l'alternativa per quella regola.

        Per passare all'utilizzo dell'azione di una regola, nella configurazione Web ACL, modifica l'istruzione della regola per il gruppo di regole e rimuovi l'Countoverride per la regola. Se gestisci l'ACL web in JSON, nell'istruzione di riferimento del gruppo di regole rimuovi la voce relativa alla regola dall'elenco. `RuleActionOverrides`
      - Web ACL: se hai modificato l'azione predefinita dell'ACL Web per i tuoi test, passa all'impostazione di produzione.

Con queste impostazioni, le nuove protezioni gestiranno il traffico web come previsto.

Quando salvi il tuo ACL web, le risorse a cui è associato utilizzeranno le tue impostazioni di produzione.

2. Monitora e ottimizza

   Per assicurarti che le richieste web vengano gestite come desideri, monitora attentamente il traffico dopo aver abilitato la nuova funzionalità. Monitorerai le metriche e i log per le azioni relative alle regole di produzione, anziché contare le azioni che stavi monitorando durante il lavoro di ottimizzazione. Continuate a monitorare e adattate il comportamento secondo necessità per adattarvi ai cambiamenti del traffico web.

Come AWS WAF funziona con le CloudFront funzionalità di Amazon

Quando crei un ACL web, puoi specificare una o più CloudFront distribuzioni che desideri AWS WAF ispezionare. AWS WAF inizia a ispezionare e gestire le richieste Web per tali distribuzioni in base ai criteri identificati nell'ACL Web. CloudFront fornisce alcune funzionalità che migliorano la funzionalità. AWS WAF Questo capitolo descrive alcuni modi in cui è possibile configurare CloudFront per creare CloudFront e AWS WAF lavorare meglio insieme.

Argomenti

- Utilizzo AWS WAF con pagine di errore CloudFront personalizzate
- Utilizzo di AWS WAF with CloudFront per le applicazioni in esecuzione sul tuo server HTTP
- Scelta dei metodi HTTP che CloudFront rispondono a

Utilizzo AWS WAF con pagine di errore CloudFront personalizzate

Per impostazione predefinita, quando AWS WAF blocca una richiesta Web in base ai criteri specificati, restituisce il codice di stato HTTP `403 (Forbidden)` a CloudFront e lo CloudFront restituisce al visualizzatore. Il visualizzatore visualizza quindi un messaggio predefinito breve e poco formattato simile al seguente:

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

È possibile ignorare questo comportamento nelle regole ACL AWS WAF Web definendo risposte personalizzate. Per ulteriori informazioni sulla personalizzazione del comportamento di risposta mediante AWS WAF le regole, consulta. Risposte personalizzate per Block le azioni

> **Note**
>
> Le risposte personalizzate utilizzando AWS WAF le regole hanno la precedenza su tutte le specifiche di risposta definite nelle pagine di errore CloudFront personalizzate.

Se preferisci visualizzare un messaggio di errore personalizzato CloudFront, possibilmente utilizzando la stessa formattazione del resto del sito Web, puoi configurare CloudFront la visualizzazione di un oggetto (ad esempio un file HTML) che contenga il tuo messaggio di errore personalizzato.

> **Note**
>
> CloudFront non è in grado di distinguere tra un codice di stato HTTP 403 restituito dall'origine e uno restituito da AWS WAF quando una richiesta viene bloccata. Ciò significa che non è possibile restituire pagine di errore personalizzate diverse a seconda delle diverse cause di un codice di stato HTTP 403.

Per ulteriori informazioni sulle pagine di errore CloudFront personalizzate, consulta Generazione di risposte di errore personalizzate nell'Amazon CloudFront Developer Guide.

Utilizzo di AWS WAF with CloudFront per le applicazioni in esecuzione sul tuo server HTTP

Quando utilizzi AWS WAF con CloudFront, puoi proteggere le tue applicazioni in esecuzione su qualsiasi server Web HTTP, che si tratti di un server Web in esecuzione su Amazon Elastic Compute Cloud (Amazon EC2) o di un server Web gestito privatamente. Puoi anche configurare in modo CloudFront da richiedere l'HTTPS tra il tuo server web CloudFront e tra i visualizzatori e. CloudFront

Richiedere HTTPS tra CloudFront e il proprio server web

Per richiedere HTTPS tra CloudFront e il tuo server web, puoi utilizzare la funzionalità di origine CloudFront personalizzata e configurare la Origin Protocol Policy e le impostazioni del nome di dominio di origine per origini specifiche. Nella CloudFront configurazione, è possibile specificare il nome DNS del server insieme alla porta e al protocollo che si desidera utilizzare CloudFront per recuperare oggetti dall'origine. È inoltre necessario assicurarsi che il certificato SSL/TLS sul server di origine personalizzato corrisponda al nome di dominio di origine configurato. Quando si utilizza il proprio server web HTTP all'esterno di AWS, è necessario utilizzare un certificato firmato da un'autorità di certificazione (CA) di terze parti affidabile, ad esempio Comodo o Symantec DigiCert. Per ulteriori informazioni sulla richiesta di HTTPS per la comunicazione tra CloudFront e il tuo server web, consulta l'argomento Richiedere HTTPS per la comunicazione tra CloudFront e la tua origine personalizzata nella Amazon CloudFront Developer Guide.

Richiedere HTTPS tra un visualizzatore e CloudFront

Per richiedere HTTPS tra i visualizzatori e CloudFront, puoi modificare la Viewer Protocol Policy per uno o più comportamenti della cache nella tua CloudFront distribuzione. Per ulteriori informazioni sull'utilizzo di HTTPS tra visualizzatori e CloudFront, consulta l'argomento Richiedere HTTPS per la comunicazione tra visualizzatori e CloudFront nella Amazon CloudFront Developer Guide. Puoi anche portare il tuo certificato SSL in modo che gli spettatori possano connettersi alla tua CloudFront distribuzione tramite HTTPS utilizzando il tuo nome di dominio, ad esempio https://www.mysite.com. Per ulteriori informazioni, consulta l'argomento Configurazione di nomi di dominio alternativi e HTTPS nella Amazon CloudFront Developer Guide.

Scelta dei metodi HTTP che CloudFront rispondono a

Quando crei una distribuzione CloudFront web Amazon, scegli i metodi HTTP che desideri CloudFront elaborare e inoltrare all'origine. Puoi scegliere tra le seguenti opzioni:

- **`GET`**, **`HEAD`** — Puoi utilizzarli CloudFront solo per recuperare oggetti dall'origine o per ottenere le intestazioni degli oggetti.
- **`GET`**,**`HEAD`**, **`OPTIONS`** — È possibile utilizzarlo CloudFront solo per recuperare oggetti dall'origine, ottenere le intestazioni degli oggetti o recuperare un elenco delle opzioni supportate dal server di origine.
- **`GET`**,**`HEAD`**,**`OPTIONS`**,,**`PUT`**, **`POSTPATCH`**, **`DELETE`** — È possibile utilizzarlo CloudFront per ottenere, aggiungere, aggiornare ed eliminare oggetti e per ottenere le intestazioni degli oggetti. Inoltre, è possibile eseguire altre `POST` operazioni come l'invio di dati da un modulo Web.

È inoltre possibile utilizzare le istruzioni delle regole di corrispondenza dei AWS WAF byte per consentire o bloccare le richieste in base al metodo HTTP, come descritto in. Istruzione regola di corrispondenza stringa Se desideri utilizzare una combinazione di metodi che CloudFront supporti, ad esempio `GET` e`HEAD`, non è necessario configurare AWS WAF per bloccare le richieste che utilizzano gli altri metodi. Se desideri consentire una combinazione di metodi che CloudFront non supporta, ad esempio, e `GET` `HEADPOST`, puoi configurare in modo che CloudFront risponda a tutti i metodi e quindi utilizzarla AWS WAF per bloccare le richieste che utilizzano altri metodi.

Per ulteriori informazioni sulla scelta dei metodi a cui CloudFront rispondere, consulta Metodi HTTP consentiti nell'argomento Valori che specifichi quando crei o aggiorni una distribuzione Web nella Amazon CloudFront Developer Guide.

Sicurezza nell'utilizzo del AWS WAF servizio

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

> **Note**
>
> Questa sezione fornisce linee guida AWS di sicurezza standard per l'utilizzo del AWS WAF servizio e delle relative AWS risorse, come ACL AWS WAF Web e gruppi di regole.
> Per informazioni sulla protezione AWS delle risorse utilizzate AWS WAF, consultate il resto della AWS WAF guida.

La sicurezza è una responsabilità condivisa tra te AWS e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. L'efficacia della nostra sicurezza è regolarmente testata e verificata da revisori di terze parti come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità applicabili AWS WAF, consulta AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e leggi e normative applicabili.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS WAF. Negli argomenti seguenti viene illustrato come eseguire la configurazione AWS WAF per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere AWS WAF le tue risorse.

Argomenti

Protezione dei dati in AWS WAF

Il modello di responsabilità AWS condivisa modello di di si applica alla protezione dei dati in AWS WAF. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.

- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori o Servizi AWS utilizzi la console, l'API AWS WAF o gli SDK. AWS CLI AWS I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

AWS WAF le entità, come gli ACL Web, i gruppi di regole e i set IP, sono crittografate quando sono inattive, tranne in alcune regioni in cui la crittografia non è disponibile, tra cui Cina (Pechino) e Cina (Ningxia). Per ogni regione vengono utilizzate chiavi di crittografia univoche.

Eliminazione delle risorse AWS WAF

Puoi eliminare le risorse che crei in AWS WAF. Consulta la guida per ogni tipo di risorsa nelle sezioni seguenti.

- Eliminazione di un ACL Web
- Eliminazione di un gruppo di regole
- Eliminazione di un set di IP
- Eliminazione di un set del modello regex

Gestione delle identità e degli accessi per AWS WAF

AWS Identity and Access Management (IAM) aiuta un Servizio AWS amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS WAF IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che AWS WAF svolgi.

Utente del servizio: se utilizzi il AWS WAF servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AWS WAF funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AWS WAF, consulta Risoluzione dei problemi di AWS WAF identità e accesso.

Amministratore del servizio: se sei responsabile delle AWS WAF risorse della tua azienda, probabilmente hai pieno accesso a AWS WAF. È tuo compito determinare a quali AWS WAF funzionalità e risorse devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con AWS WAF, consultaCome AWS WAF funziona con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a AWS WAF. Per visualizzare esempi di policy AWS WAF basate sull'identità che puoi utilizzare in IAM, consulta. Esempi di policy basate su identità per AWS WAF

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per

effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

- Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'azione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruoli IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per sapere come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come AWS WAF funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS WAF, scopri con quali funzionalità IAM è disponibile l'uso AWS WAF.

Funzionalità IAM che puoi utilizzare con AWS WAF

Funzionalità IAM	AWS WAF supporto
Policy basate su identità	Sì
Policy basate su risorse	Sì
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

Per avere una panoramica di alto livello su come AWS WAF e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per AWS WAF

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Per visualizzare esempi di politiche basate sull' AWS WAF identità, vedere. Esempi di policy basate su identità per AWS WAF

Politiche basate sulle risorse all'interno AWS WAF

Supporta le policy basate su risorse	Sì

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account

a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

AWS WAF utilizza politiche basate sulle risorse per supportare la condivisione di gruppi di regole tra gli account. Puoi condividere un gruppo di regole di tua proprietà con un altro AWS account fornendo le impostazioni delle politiche basate sulle risorse alla chiamata AWS WAF API o a una chiamata CLI `PutPermissionPolicy` o SDK equivalente. Per ulteriori informazioni, inclusi esempi e collegamenti alla documentazione per le altre lingue disponibili, PutPermissionPolicyconsulta l'API Reference. AWS WAF Questa funzionalità non è disponibile tramite altri mezzi, come la console o AWS CloudFormation.

Azioni politiche per AWS WAF

Supporta le azioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di AWS WAF azioni e autorizzazioni per ciascuna di esse, consulta Actions defined by AWS WAF V2 nel Service Authorization Reference.

Le azioni politiche in AWS WAF uso utilizzano il seguente prefisso prima dell'azione:

```
wafv2
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "wafv2:action1",
      "wafv2:action2"
         ]
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni AWS WAF che iniziano con`List`, includi la seguente azione:

```
"Action": "wafv2:List*"
```

Per visualizzare esempi di politiche AWS WAF basate sull'identità, vedere. Esempi di policy basate su identità per AWS WAF

Azioni che richiedono impostazioni di autorizzazioni aggiuntive

Alcune azioni richiedono autorizzazioni che non possono essere descritte completamente in Azioni definite dalla AWS WAF V2 nel Service Authorization Reference. Questa sezione fornisce informazioni aggiuntive sulle autorizzazioni.

Argomenti

- Autorizzazioni per AssociateWebACL
- Autorizzazioni per DisassociateWebACL
- Autorizzazioni per GetWebACLForResource
- Autorizzazioni per ListResourcesForWebACL

Autorizzazioni per **`AssociateWebACL`**

Questa sezione elenca le autorizzazioni necessarie per associare un ACL Web a una risorsa utilizzando l'azione. AWS WAF `AssociateWebACL`

Per CloudFront le distribuzioni Amazon, invece di questa azione, usa l' CloudFront azione`UpdateDistribution`. Per informazioni, UpdateDistributionconsulta Amazon CloudFront API Reference.

API REST di Amazon API Gateway

Richiede l'autorizzazione per chiamare API Gateway `SetWebACL` sul tipo di risorsa API REST e per chiamare AWS WAF `AssociateWebACL` un 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/*"
    ]
}
```

Application Load Balancer

Richiede l'autorizzazione per eseguire `elasticloadbalancing:SetWebACL` un'azione sul tipo di risorsa Application Load Balancer e per AWS WAF `AssociateWebACL` richiamare un 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

Richiede l'autorizzazione per richiamare AWS AppSync `SetWebACL` il tipo di risorsa GraphQL API e per richiamare un 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/*"
    ]
}
```

Bacino d'utenza di Amazon Cognito

Richiede l'autorizzazione per richiamare l'`AssociateWebACL`azione Amazon Cognito sul tipo di risorsa del pool di utenti e per AWS WAF `AssociateWebACL` richiamare un 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 servizio

Richiede l'autorizzazione per richiamare l'`AssociateWebACL`azione App Runner sul tipo di risorsa del servizio App Runner e per AWS WAF `AssociateWebACL` richiamare un 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 Istanza Verified Access

Richiede l'autorizzazione per eseguire l'`ec2:AssociateVerifiedAccessInstanceWebAc`lazione sul tipo di risorsa dell'istanza Verified Access e per richiamare AWS WAF `AssociateWebACL` un 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/*"
    ]
}
```

Autorizzazioni per **`DisassociateWebACL`**

Questa sezione elenca le autorizzazioni necessarie per dissociare un ACL Web da una risorsa utilizzando l'azione. AWS WAF `DisassociateWebACL`

Per CloudFront le distribuzioni Amazon, anziché questa azione, utilizza l' CloudFront azione `UpdateDistribution` con un ID ACL Web vuoto. Per informazioni, UpdateDistributionconsulta Amazon CloudFront API Reference.

API REST di Amazon API Gateway

Richiede l'autorizzazione per chiamare API Gateway `SetWebACL` sul tipo di risorsa API REST. Non richiede l'autorizzazione per chiamare AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL",
```

```
    "Effect": "Allow",
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}
```

Application Load Balancer

Richiede l'autorizzazione per eseguire l'`elasticloadbalancing:SetWebACL`azione sul tipo di risorsa Application Load Balancer. Non richiede l'autorizzazione per chiamare AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:SetWebACL"
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

AWS AppSync API GraphQL

Richiede l'autorizzazione per richiamare AWS AppSync `SetWebACL` il tipo di risorsa GraphQL API. Non richiede l'autorizzazione per chiamare AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Bacino d'utenza di Amazon Cognito

Richiede l'autorizzazione per richiamare l'`DisassociateWebACL`azione Amazon Cognito sul tipo di risorsa del pool di utenti e per effettuare la chiamata. 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 servizio

Richiede l'autorizzazione per richiamare l'`DisassociateWebACL`azione App Runner sul tipo di risorsa del servizio App Runner e per effettuare la chiamata. 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 Istanza Verified Access

Richiede l'autorizzazione per avviare l'`ec2:DisassociateVerifiedAccessInstanceWebAc`lazione sul tipo di risorsa dell'istanza Verified Access e per effettuare la chiamata 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/*"
    ]
}
```

Autorizzazioni per **`GetWebACLForResource`**

Questa sezione elenca le autorizzazioni necessarie per ottenere l'ACL Web per una risorsa protetta utilizzando l'azione AWS WAF . `GetWebACLForResource`

Per CloudFront le distribuzioni Amazon, invece di questa azione, usa l' CloudFront azione`GetDistributionConfig`. Per informazioni, GetDistributionConfigconsulta Amazon CloudFront API Reference.

> **Note**
>
> `GetWebACLForResource`richiede l'autorizzazione per chiamare`GetWebACL`. In questo contesto, AWS WAF viene utilizzato `GetWebACL` solo per verificare che l'account disponga dell'autorizzazione necessaria per accedere all'ACL Web che `GetWebACLForResource` restituisce. Quando chiami`GetWebACLForResource`, potresti ricevere un errore che indica

che il tuo account non è autorizzato a eseguire operazioni `wafv2:GetWebACL` sulla risorsa. AWS WAF non aggiunge questo tipo di errore alla cronologia degli AWS CloudTrail eventi.

API REST di Amazon API Gateway, Application Load Balancer e API GraphQL AWS AppSync

Richiedi l'autorizzazione per chiamare AWS WAF `GetWebACLForResource` e `GetWebACL` per un ACL web.

```
{
    "Sid": "GetWebACLForResource",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

Bacino d'utenza di Amazon Cognito

Richiede l'autorizzazione per richiamare l'`GetWebACLForResource`azione Amazon Cognito sul tipo di risorsa del pool di utenti e per chiamare AWS WAF `GetWebACLForResource` e. `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 servizio

Richiede l'autorizzazione per richiamare l'`DescribeWebAclForService`azione App Runner sul tipo di risorsa del servizio App Runner e per chiamare AWS WAF `GetWebACLForResource` e. `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 Istanza Verified Access

Richiede l'autorizzazione per avviare l'`ec2:GetVerifiedAccessInstanceWebAcl`azione sul tipo di risorsa dell'istanza Verified Access e per chiamare AWS WAF `GetWebACLForResource` e`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/*"
    ]
}
```

Autorizzazioni per **`ListResourcesForWebACL`**

Questa sezione elenca le autorizzazioni necessarie per recuperare l'elenco delle risorse protette per un ACL Web utilizzando l'azione. AWS WAF `ListResourcesForWebACL`

Per CloudFront le distribuzioni Amazon, invece di questa azione, usa l' CloudFront azione`ListDistributionsByWebACLId`. Per informazioni, consulta ListDistributionsByWebAClid nell'Amazon CloudFront API Reference.

API REST di Amazon API Gateway, Application Load Balancer e API GraphQL AWS AppSync

Richiedi l'autorizzazione AWS WAF `ListResourcesForWebACL` per richiedere un ACL web.

```
{
    "Sid": "ListResourcesForWebACL",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

Bacino d'utenza di Amazon Cognito

Richiede l'autorizzazione per richiamare l'`ListResourcesForWebACL`azione Amazon Cognito sul tipo di risorsa del pool di utenti e per effettuare la chiamata. AWS WAF `ListResourcesForWebACL`

```
{
    "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 servizio

Richiede l'autorizzazione per richiamare l'`ListAssociatedServicesForWebAc`lazione App Runner sul tipo di risorsa del servizio App Runner e per effettuare la chiamata. 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 Istanza Verified Access

Richiede l'autorizzazione per avviare l'`ec2:DescribeVerifiedAccessInstanceWebAclAssociations`azione sul tipo di risorsa dell'istanza Verified Access e per effettuare la chiamata AWS WAF `ListResourcesForWebACL`.

```
{
    "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/*"
    ]
}
```

Risorse politiche per AWS WAF

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare l'elenco dei tipi di AWS WAF risorse e i relativi ARN, vedere Resources defined by AWS WAF V2 nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, vedere Azioni definite dalla AWS WAF V2. Per consentire o negare l'accesso a un sottoinsieme di AWS WAF risorse, includi l'ARN della risorsa nell'`resource`elemento della tua politica.

Gli ARN delle AWS WAF `wafv2` risorse hanno il seguente formato:

```
arn:partition:wafv2:region:account-id:scope/resource-type/resource-name/resource-id
```

Per informazioni generali sulle specifiche ARN, consulta Amazon Resource Names (ARNs) nel. Riferimenti generali di Amazon Web Services

Di seguito sono elencati i requisiti specifici degli ARN delle risorse: `wafv2`

- *`regione`*: Per AWS WAF le risorse che usi per proteggere CloudFront le distribuzioni Amazon, imposta questa opzione su. `us-east-1` Altrimenti, impostala sulla regione che stai utilizzando con le tue risorse regionali protette.
- *`ambito`*: imposta l'ambito `global` per l'utilizzo con una CloudFront distribuzione Amazon o `regional` per l'utilizzo con una qualsiasi delle risorse regionali AWS WAF supportate. Le risorse regionali sono un'API REST di Amazon API Gateway, un'Application Load Balancer, un'API GraphQL AWS AppSync , un pool di utenti Amazon Cognito, un AWS App Runner servizio e un'istanza Verified Access. AWS
- *`tipo di risorsa`*: specifica uno dei seguenti valori:,,, o. `webacl` `rulegroup` `ipset` `regexpatternset` `managedruleset`

- *resource-name*: specifica il nome che hai assegnato alla AWS WAF risorsa o specifica un wildcard (*) per indicare tutte le risorse che soddisfano le altre specifiche dell'ARN. È necessario specificare il nome e l'ID della risorsa o specificare un carattere jolly per entrambi.
- *resource-id*: specifica l'ID della AWS WAF risorsa o specifica un wildcard (*) per indicare tutte le risorse che soddisfano le altre specifiche dell'ARN. È necessario specificare il nome e l'ID della risorsa o specificare un carattere jolly per entrambi.

Ad esempio, il seguente ARN specifica tutte le ACL Web con ambito regionale per l'account `111122223333` nella regione `us-west-1`:

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

Il seguente ARN specifica il gruppo di regole denominato `MyIPManagementRuleGroup` con ambito globale per l'account `111122223333` in Region: `us-east-1`

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

Per visualizzare esempi di politiche basate sull' AWS WAF identità, vedere. Esempi di policy basate su identità per AWS WAF

Chiavi relative alle condizioni delle politiche per AWS WAF

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione

logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Inoltre, AWS WAF supporta le seguenti chiavi di condizione che puoi utilizzare per fornire filtri dettagliati per le tue politiche IAM:

- wafv2: LogDestinationResource

  Questa chiave condizionale richiede una specifica Amazon Resource Name (ARN) per la destinazione di registrazione. Si tratta dell'ARN fornito per la destinazione di registrazione quando si utilizza la chiamata API REST. `PutLoggingConfiguration`

  È possibile specificare in modo esplicito un ARN e specificare il filtraggio per l'ARN. L'esempio seguente specifica il filtraggio per gli ARN dei bucket Amazon S3 che hanno una posizione e un prefisso specifici.

  ```
  "Condition": { "ArnLike": { "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-suffix/custom-prefix/*" } }
  ```

- wafv2: LogScope

  Questa chiave condizionale definisce l'origine della configurazione di registrazione in una stringa. Attualmente, è sempre impostato sul valore predefinito di`Customer`, che indica che la destinazione di registrazione è di proprietà e gestita dall'utente.

Per visualizzare un elenco di chiavi di AWS WAF condizione, consulta Condition keys for AWS WAF V2 nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, vedi Azioni definite da AWS WAF V2.

Per visualizzare esempi di politiche AWS WAF basate sull'identità, vedere. Esempi di policy basate su identità per AWS WAF

ACL in AWS WAF

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con AWS WAF

Supporta ABAC (tag nelle policy)	Parziale

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con AWS WAF

Supporta le credenziali temporanee	Sì

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Inoltra sessioni di accesso al servizio AWS WAF

Supporta sessioni di accesso diretto (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Inoltro sessioni di accesso.

Ruoli di servizio per AWS WAF

Supporta i ruoli di servizio	Sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità. AWS WAF Modifica i ruoli di servizio solo quando viene AWS WAF fornita una guida in tal senso.

Ruoli collegati ai servizi per AWS WAF

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati in Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione di ruoli AWS WAF collegati ai servizi, consulta. Utilizzo di ruoli collegati ai servizi per AWS WAF

Esempi di policy basate su identità per AWS WAF

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse AWS WAF . Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS l'API. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da AWS WAF, incluso il formato degli ARN per ciascun tipo di risorsa, vedere Azioni, risorse e chiavi di condizione per AWS WAF V2 nel Service Authorization Reference.

Argomenti

- Best practice per le policy

- Utilizzo della console di AWS WAF
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Concedi l'accesso in sola lettura a, e AWS WAF CloudFront CloudWatch
- Concedi l'accesso completo a AWS WAF, e CloudFront CloudWatch
- Concedi l'accesso a un singolo Account AWS
- Concedi l'accesso a una singola ACL web
- Concedi l'accesso CLI a un ACL Web e a un gruppo di regole

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare AWS WAF risorse nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso ad azioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100

controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.

- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console di AWS WAF

Per accedere alla AWS WAF console, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle AWS WAF risorse del tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano utilizzare la AWS WAF console, allega anche almeno la policy AWS WAF `AWSWAFConsoleReadOnlyAccess` AWS gestita alle entità. Per informazioni su questa politica gestita, vedereAWS politica gestita: AWSWAFConsoleReadOnlyAccess. Per ulteriori informazioni su come allegare una policy gestita a un utente, consulta Adding permissions to a user nella IAM User Guide.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa policy include le autorizzazioni per completare questa azione sulla console o utilizzando l'API or a livello di codice. AWS CLI 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": "*"
        }
    ]
}
```

Concedi l'accesso in sola lettura a, e AWS WAF CloudFront CloudWatch

La seguente politica garantisce agli utenti l'accesso in sola lettura alle AWS WAF risorse, alle distribuzioni CloudFront Web di Amazon e ai parametri Amazon. CloudWatch È utile per gli utenti che necessitano dell'autorizzazione per visualizzare le impostazioni in AWS WAF condizioni, regole e ACL Web per vedere quale distribuzione è associata a un ACL Web e per monitorare le metriche e un campione di richieste in esso. CloudWatch Questi utenti non possono creare, aggiornare o eliminare le risorse 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": "*"
      }
   ]
}
```

Concedi l'accesso completo a AWS WAF, e CloudFront CloudWatch

La seguente politica consente agli utenti di eseguire qualsiasi AWS WAF operazione, eseguire qualsiasi operazione sulle distribuzioni CloudFront Web e monitorare le metriche e un campione di richieste in. CloudWatch È utile per gli utenti che sono AWS WAF amministratori.

```
{
   "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": "*"
      }
```

```
   ]
}
```

Consigliamo vivamente di configurare l'autenticazione a più fattori (MFA) per gli utenti che dispongono di autorizzazioni amministrative. Per ulteriori informazioni, consulta Using Multi-Factor Authentication (MFA) Devices AWS with nella IAM User Guide.

Concedi l'accesso a un singolo Account AWS

Questa politica concede le seguenti autorizzazioni all'account 444455556666:

- Accesso completo a tutte le AWS WAF operazioni e le risorse.
- Accesso in lettura e aggiornamento a tutte le CloudFront distribuzioni, che consente di associare ACL Web e CloudFront distribuzioni.
- Accesso in lettura a tutte le CloudWatch metriche e alle statistiche metriche, in modo da poter visualizzare CloudWatch i dati e un campione di richieste nella console. 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": [
            "*"
         ]
      }
   ]
}
```

Concedi l'accesso a una singola ACL web

La seguente politica consente agli utenti di eseguire qualsiasi AWS WAF operazione tramite la console su un ACL Web specifico dell'account. 444455556666

```
{
    "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": [
                "*"
            ]
        }
    ]
}
```

Concedi l'accesso CLI a un ACL Web e a un gruppo di regole

La seguente politica consente agli utenti di eseguire qualsiasi AWS WAF operazione tramite la CLI su un ACL Web specifico e un gruppo di regole specifico nell'account. 444455556666

```
{
   "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 seguente politica consente agli utenti di eseguire qualsiasi AWS WAF operazione tramite la console su un ACL Web specifico dell'account. `444455556666`

```
{
    "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 politiche gestite per AWS WAF

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AWS politica gestita: AWSWAFReadOnlyAccess

Questa politica concede autorizzazioni di sola lettura che consentono agli utenti di accedere a AWS WAF risorse e risorse per servizi integrati, come Amazon, Amazon API CloudFront Gateway, Application Load Balancer, AWS AppSync Amazon Cognito e Verified Access. AWS App Runner AWS Puoi collegare questa policy alle tue identità IAM. AWS WAF associa inoltre questa policy a un ruolo di servizio che consente di AWS WAF eseguire azioni per tuo conto.

Per i dettagli su questa politica, consulta AWSWAFReadOnlyAccessnella console IAM.

AWS politica gestita: AWSWAFFullAccess

Questa politica garantisce l'accesso completo a AWS WAF risorse e risorse per servizi integrati, come Amazon, Amazon API Gateway CloudFront, Application Load Balancer AWS AppSync, Amazon Cognito e Verified Access. AWS App Runner AWS Puoi collegare questa policy alle tue identità IAM. AWS WAF associa inoltre questa policy a un ruolo di servizio che consente di AWS WAF eseguire azioni per tuo conto.

Per i dettagli su questa politica, consulta AWSWAFFullAccessnella console IAM.

AWS politica gestita: AWSWAFConsoleReadOnlyAccess

Questa politica concede autorizzazioni di sola lettura alla AWS WAF console, che include risorse per AWS WAF e per servizi integrati, come Amazon, Amazon API CloudFront Gateway, Application Load Balancer, AWS AppSync Amazon Cognito e Verified Access. AWS App Runner AWS Puoi collegare questa policy alle tue identità IAM. AWS WAF associa inoltre questa policy a un ruolo di servizio che consente di AWS WAF eseguire azioni per tuo conto.

Per i dettagli su questa politica, consulta AWSWAFConsoleReadOnlyAccessnella console IAM.

AWS politica gestita: AWSWAFConsoleFullAccess

Questa politica garantisce l'accesso completo alla AWS WAF console, che include risorse per AWS WAF e per servizi integrati, come Amazon, Amazon API Gateway CloudFront, Application Load Balancer AWS AppSync, Amazon Cognito e Verified Access. AWS App Runner AWS Puoi collegare questa policy alle tue identità IAM. AWS WAF associa inoltre questa policy a un ruolo di servizio che consente di AWS WAF eseguire azioni per tuo conto.

Per i dettagli su questa politica, consulta AWSWAFConsoleFullAccessnella console IAM.

AWS WAF aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AWS WAF da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei AWS WAF documenti all'indirizzo. Cronologia dei documenti

Policy	Descrizione della modifica	Data
`AWSWAFFullAccess` Questa politica consente di AWS WAF gestire AWS le risorse per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati.	Autorizzazioni estese per aggiungere istanze AWS Verified Access ai tipi di risorse con cui puoi proteggerti. AWS WAF	2023-06-17

Policy	Descrizione della modifica	Data
Dettagli nella console IAM: AWSWAFFullAccess.		
`AWSWAFReadOnlyAccess` Questa politica consente di gestire AWS le risorse AWS WAF per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFReadOnlyAccess.	Autorizzazioni estese per aggiungere istanze AWS Verified Access ai tipi di risorse con cui puoi proteggerti. AWS WAF	2023-06-17
`AWSWAFConsoleFullAccess` Questa policy consente di AWS WAF gestire le risorse AWS della console e altre AWS risorse per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFConsoleFullAccess.	Autorizzazioni estese per aggiungere istanze AWS Verified Access ai tipi di risorse con cui puoi proteggerti. AWS WAF	2023-06-17

Policy	Descrizione della modifica	Data
`AWSWAFConsoleReadOnlyAccess` Questa policy consente di AWS WAF gestire le risorse AWS della console e altre AWS risorse per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFConsoleReadOnlyAccess.	Autorizzazioni estese per aggiungere istanze AWS Verified Access ai tipi di risorse con cui puoi proteggerti. AWS WAF	2023-06-17
`AWSWAFFullAccess` Questa politica consente di gestire AWS le risorse AWS WAF per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFFullAccess.	Autorizzazioni estese per correggere le impostazioni di accesso ai AWS App Runner servizi.	2023-06-06
`AWSWAFReadOnlyAccess` Questa politica consente di gestire AWS le risorse AWS WAF per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFReadOnlyAccess.	Autorizzazioni estese per correggere le impostazioni di accesso ai AWS App Runner servizi.	2023-06-06

Policy	Descrizione della modifica	Data
`AWSWAFConsoleFullAccess` Questa politica consente di AWS WAF gestire le risorse AWS della console e altre AWS risorse per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFConsoleFullAccess.	Autorizzazioni estese per correggere le impostazioni di accesso ai AWS App Runner servizi.	2023-06-06
`AWSWAFConsoleReadOnlyAccess` Questa politica consente di AWS WAF gestire le risorse AWS della console e altre AWS risorse per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFConsoleReadOnlyAccess.	Autorizzazioni estese per correggere le impostazioni di accesso ai AWS App Runner servizi.	2023-06-06

Policy	Descrizione della modifica	Data
`AWSWAFFullAccess` Questa politica consente di gestire AWS le risorse AWS WAF per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFFullAccess.	Autorizzazioni estese per aggiungere AWS App Runner servizi ai tipi di risorse con AWS WAF cui puoi proteggerti.	2023-03-30
`AWSWAFReadOnlyAccess` Questa politica consente di gestire AWS le risorse AWS WAF per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFReadOnlyAccess.	Autorizzazioni estese per aggiungere AWS App Runner servizi ai tipi di risorse con AWS WAF cui puoi proteggerti.	2023-03-30
`AWSWAFConsoleFullAccess` Questa politica consente di AWS WAF gestire le risorse AWS della console e altre AWS risorse per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFConsoleFullAccess.	Autorizzazioni estese per aggiungere AWS App Runner servizi ai tipi di risorse con AWS WAF cui puoi proteggerti.	2023-03-30

Policy	Descrizione della modifica	Data
`AWSWAFConsoleReadOnlyAccess` Questa politica consente di AWS WAF gestire le risorse AWS della console e altre AWS risorse per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFConsoleReadOnlyAccess.	Autorizzazioni estese per aggiungere AWS App Runner servizi ai tipi di risorse con AWS WAF cui puoi proteggerti.	2023-03-30
`AWSWAFFullAccess` Questa politica consente di gestire AWS le risorse AWS WAF per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFFullAccess.	Autorizzazioni estese per aggiungere pool di utenti Amazon Cognito ai tipi di risorse con cui puoi proteggerti. AWS WAF	25/08/2022
`AWSWAFReadOnlyAccess` Questa politica consente di gestire AWS le risorse AWS WAF per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFReadOnlyAccess.	Autorizzazioni estese per aggiungere pool di utenti Amazon Cognito ai tipi di risorse con cui puoi proteggerti. AWS WAF	25/08/2022

Policy	Descrizione della modifica	Data
`AWSWAFConsoleFullAccess` Questa politica consente di AWS WAF gestire le risorse AWS della console e altre AWS risorse per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFConsoleFullAccess.	Autorizzazioni estese per aggiungere pool di utenti Amazon Cognito ai tipi di risorse con cui puoi proteggerti. AWS WAF	25/08/2022
`AWSWAFConsoleReadOnlyAccess` Questa politica consente di AWS WAF gestire le risorse AWS della console e altre AWS risorse per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFConsoleReadOnlyAccess.	Autorizzazioni estese per aggiungere pool di utenti Amazon Cognito ai tipi di risorse con cui puoi proteggerti. AWS WAF	25/08/2022

Policy	Descrizione della modifica	Data
`AWSWAFFullAccess` Questa politica consente di gestire AWS le risorse AWS WAF per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFFullAccess.	Sono state corrette le impostazioni delle autorizzazioni per la consegna dei log per Amazon Simple Storage Service (Amazon S3) e Amazon Logs. CloudWatch Questa modifica risolve gli errori di accesso negato che si verificavano durante la configurazione della registrazione. Per informazioni sulla registrazione del traffico ACL Web, consulta. Registrazione del traffico AWS WAF ACL Web	2022-01-11
`AWSWAFConsoleFullAccess` Questa politica consente di AWS WAF gestire le risorse AWS della console e altre AWS risorse per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFConsoleFullAccess.	Sono state corrette le impostazioni delle autorizzazioni per la consegna dei log per Amazon Simple Storage Service (Amazon S3) e Amazon Logs. CloudWatch Questa modifica risolve gli errori di accesso che si verificavano durante la configurazione della registrazione. Per informazioni sulla registrazione del traffico ACL Web, consulta. Registrazione del traffico AWS WAF ACL Web	2022-01-11

Policy	Descrizione della modifica	Data
`AWSWAFFullAccess` Questa politica consente di gestire AWS le risorse AWS WAF per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFFullAccess.	Aggiunte nuove autorizzazioni per opzioni di registrazione estese. Questa modifica consente di AWS WAF accedere alle destinazioni di registrazione aggiuntive Amazon Simple Storage Service (Amazon S3) e Amazon Logs. CloudWatch Per informazioni sulla registrazione del traffico Web ACL, consulta. Registrazione del traffico AWS WAF ACL Web	2021-11-15
`AWSWAFConsoleFullAccess` Questa policy consente di AWS WAF gestire le risorse AWS della console e altre AWS risorse per conto dell'utente all'interno AWS WAF e all'interno di servizi integrati. Dettagli nella console IAM: AWSWAFConsoleFullAccess.	Aggiunte nuove autorizzazioni per opzioni di registrazione estese. Questa modifica consente di AWS WAF accedere alle destinazioni di registrazione aggiuntive Amazon Simple Storage Service (Amazon S3) e Amazon Logs. CloudWatch Per informazioni sulla registrazione del traffico Web ACL, consulta. Registrazione del traffico AWS WAF ACL Web	2021-11-15
AWS WAF ha iniziato a tenere traccia delle modifiche	AWS WAF ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	2021-3-01

Risoluzione dei problemi di AWS WAF identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con un AWS WAF IAM.

Argomenti

Non sono autorizzato a eseguire alcuna azione in AWS WAF

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `wafv2:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 wafv2:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `wafv2:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a AWS WAF.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in AWS WAF. Tuttavia, l'operazione richiede che

il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS WAF risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS WAF supporta queste funzionalità, consultaCome AWS WAF funziona con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Utilizzo di ruoli collegati ai servizi per AWS WAF

AWS WAF utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. AWS WAF I ruoli collegati ai servizi sono predefiniti AWS WAF e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione AWS WAF perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS WAF definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. AWS WAF Le autorizzazioni definite includono policy di attendibilità e di autorizzazioni. Questa policy delle autorizzazioni non può essere collegata ad alcun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. In questo modo proteggi AWS WAF le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per AWS WAF

AWS WAF utilizza il ruolo collegato al servizio. `AWSServiceRoleForWAFV2Logging`

AWS WAF utilizza questo ruolo collegato al servizio per scrivere log su Amazon Data Firehose. Questo ruolo viene utilizzato solo se abiliti l'accesso. AWS WAF Per ulteriori informazioni, consulta Registrazione del traffico AWS WAF ACL Web.

Ai fini dell'assunzione del ruolo `AWSServiceRoleForWAFV2Logging`, il ruolo collegato ai servizi `wafv2.amazonaws.com`considera attendibile il servizio.

Le politiche di autorizzazione del ruolo consentono di AWS WAF completare le seguenti azioni sulle risorse specificate:

- Azione: `firehose:PutRecord` e `firehose:PutRecordBatch` su Amazon Data Firehose risorse di flusso di dati con un nome che inizia con "aws-waf-logs-». Ad esempio, `aws-waf-logs-us-east-2-analytics`.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per AWS WAF

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando abiliti AWS WAF l'accesso o AWS Management Console effettui una `PutLoggingConfiguration` richiesta nella AWS WAF CLI o nell'API AWS WAF , crea AWS WAF automaticamente il ruolo collegato al servizio.

È necessario disporre dell'autorizzazione `iam:CreateServiceLinkedRole` per attivare la registrazione.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando abiliti la AWS WAF registrazione, AWS WAF crea nuovamente il ruolo collegato al servizio per te.

Modifica di un ruolo collegato ai servizi per AWS WAF

AWS WAF non consente di modificare il ruolo collegato al `AWSServiceRoleForWAFV2Logging` servizio. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per AWS WAF

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

> **Note**
>
> Se il AWS WAF servizio utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare AWS WAF le risorse utilizzate da **`AWSServiceRoleForWAFV2Logging`**

1. Sulla AWS WAF console, rimuovi la registrazione da ogni ACL Web. Per ulteriori informazioni, consulta Registrazione del traffico AWS WAF ACL Web.
2. Utilizzando l'API o l'interfaccia CLI, inviare una richiesta di `DeleteLoggingConfiguration` per ogni ACL Web che ha la registrazione attivata. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API AWS WAF.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Usa la console IAM, la CLI IAM oppure l'API IAM per eliminare il ruolo collegato ai servizi `AWSServiceRoleForWAFV2Logging`. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi AWS WAF

AWS WAF supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Endpoint e quote per AWS WAF.

Registrazione e monitoraggio AWS WAF

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle AWS WAF AWS soluzioni esistenti. È necessario raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. AWS fornisce diversi strumenti per monitorare le AWS WAF risorse e rispondere a potenziali eventi:

CloudWatch Allarmi Amazon

Utilizzando gli CloudWatch allarmi, osservi una singola metrica per un periodo di tempo specificato. Se la metrica supera una determinata soglia, CloudWatch invia una notifica a un argomento o una policy di Amazon SNS. AWS Auto Scaling Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch.

AWS CloudTrail registri

CloudTrail fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in AWS WAF. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare a quale richiesta è stata inviata AWS WAF, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi. Per ulteriori informazioni, consulta Registrazione delle chiamate API di AWS CloudTrail con.

AWS WAF registrazione del traffico web ACL

AWS WAF offre la registrazione del traffico analizzato dagli ACL Web. I log includono informazioni come l'ora in cui è AWS WAF stata ricevuta la richiesta dalla AWS risorsa protetta, informazioni dettagliate sulla richiesta e l'impostazione dell'azione per la regola a cui corrisponde la richiesta. Per ulteriori informazioni, consulta Registrazione del traffico AWS WAF ACL Web.

Convalida della conformità per AWS WAF

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono i passaggi per l'implementazione di ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

  > **Note**
  >
  > Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Evaluating Resources with Rules nella AWS Config Developer Guide: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e

verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.

- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente AWS l'utilizzo per semplificare la gestione dei rischi e la conformità alle normative e agli standard di settore.

Resilienza in AWS WAF

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

Sicurezza dell'infrastruttura nell' AWS WAF

In quanto servizio gestito, AWS WAF è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere AWS WAF attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

AWS WAF quote

> **Note**
>
> Questa è la versione più recente di AWS WAF. Per AWS WAF Classic, vediAWS WAF Classico.

AWS WAF è soggetto alle seguenti quote (precedentemente denominate limiti). Queste quote sono le stesse per tutte le regioni in cui è disponibile. AWS WAF Ogni regione è soggetta singolarmente a queste quote: le quote non sono cumulative tra regioni.

AWS WAF ha quote predefinite sul numero massimo di entità che puoi avere per account. È possibile richiedere un aumento di queste quote.

Risorsa	Quota predefinita per account per regione
Numero massimo di ACL Web	100
Numero massimo di gruppi di regole	100
Numero massimo di set IP	100
Numero massimo di richieste al secondo per ACL Web	25.000
Numero massimo di intestazioni di richiesta personalizzate per ACL Web o gruppo di regole	100
Numero massimo di intestazioni di risposta personalizzate per ACL Web o gruppo di regole	100
Numero massimo di corpi di risposta personalizzati per ACL Web o gruppo di regole	50
Numero massimo di domini token in un elenco di domini di token ACL Web	10

Il numero massimo di richieste al secondo (RPS) consentito CloudFront è impostato CloudFront e descritto nella Guida per AWS WAF gli CloudFront sviluppatori.

AWS WAF prevede quote fisse per le seguenti impostazioni di entità per account e regione. Queste quote non possono essere modificate.

Risorsa	Quota per account per regione
Numero massimo di unità di capacità ACL Web (WCU) per ACL web*	5.000
Numero massimo di WCU per gruppo di regole	5.000
Numero massimo di istruzioni di riferimento per gruppo di regole. In un gruppo di regole, un'istruzione di riferimento può fare riferimento a un set IP o a un set di pattern regex.	50
Numero massimo di istruzioni di riferimento per ACL web. In un ACL Web, un'istruzione di riferimento può fare riferimento a un gruppo di regole, un set IP o un set di pattern regex.	50
Numero massimo di indirizzi IP in notazione CIDR per set IP	10.000
Numero massimo di regole basate sulla velocità per ACL web	10
Numero massimo di regole basate sulla tariffa per gruppo di regole	4
Frequenza di richiesta minima che può essere definita per una regola basata sulla frequenza	100
Numero massimo di indirizzi IP univoci a cui è possibile limitare la velocità per regola basata sulla velocità	10.000
Numero massimo di caratteri in un'istruzione String Match	200
Numero massimo di caratteri in ogni modello regex	200
Numero massimo di modelli regex univoci per set di espressioni regolari	10
Numero massimo di set regex	10
Dimensione massima del corpo di una richiesta Web che può essere ispezionato per l'Application Load AWS AppSync Balancer e le protezioni	8 KB

Risorsa	Quota per account per regione
Dimensione massima del corpo di una richiesta Web che può essere ispezionato CloudFront, API Gateway, Amazon Cognito, App Runner e protezioni Verified Access **	64 KB
Numero massimo di trasformazioni di testo per dichiarazione di regola	10
Dimensione massima del contenuto del corpo di risposta personalizzato per una singola definizione di risposta personalizzata	4 KB
Numero massimo di intestazioni personalizzate per una singola definizione di risposta personalizzata	10
Numero massimo di intestazioni personalizzate per una singola definizione di richiesta personalizzata	10
Dimensione massima combinata di tutto il contenuto del corpo di risposta per un singolo gruppo di regole o un singolo ACL web	50 KB

*L'utilizzo di più di 1.500 WCU in un ACL Web comporta costi superiori al prezzo base dell'ACL Web. Per ulteriori informazioni, consulta AWS WAF unità di capacità Web ACL (WCU) e Prezzi di AWS WAF.

**Per impostazione predefinita, il limite di body inspection è impostato su 16 KB per CloudFront le risorse API Gateway, Amazon Cognito, App Runner e Verified Access, ma puoi aumentarlo per ognuna di queste risorse nella configurazione Web ACL, fino al massimo indicato. Per ulteriori informazioni, consulta Gestione dei limiti di dimensione delle ispezioni corporee.

AWS WAF prevede le seguenti quote fisse di chiamate per account per regione. Queste quote si applicano al totale delle chiamate al servizio tramite qualsiasi mezzo disponibile, inclusi la console, l'interfaccia a riga di comando (CLI), AWS CloudFormation, l'API REST e gli SDK. Queste quote non possono essere modificate.

Tipo di chiamata	Quota per account per regione
Numero massimo di chiamate a `AssociateWebACL`	Una richiesta ogni 2 secondi
Numero massimo di chiamate a `DisassociateWebACL`	Una richiesta ogni 2 secondi
Numero massimo di chiamate a `GetWebACLForResource`	Una richiesta al secondo
Numero massimo di chiamate a `ListResourcesForWebACL`	Una richiesta al secondo
Numero massimo di chiamate a qualsiasi operazione singola `Get` o `List`, se per l'operazione non è definita una quota diversa	Cinque richieste al secondo
Numero massimo di chiamate a qualsiasi operazione singola `Create`, `Put`, o `Update`, se per l'operazione non è definita una quota diversa	Una richiesta al secondo

Migrazione delle risorse AWS WAF Classic a AWS WAF

Questa sezione fornisce indicazioni per la migrazione delle regole e degli ACL web da AWS WAF Classic a. AWS WAF AWS WAF è stato rilasciato a novembre 2019. Se hai creato risorse come regole e ACL Web utilizzando AWS WAF Classic, devi utilizzarle utilizzando AWS WAF Classic o migrarle all'ultima versione.

Prima di iniziare il lavoro di migrazione, acquisisci familiarità con AWS WAF questa lettura. AWS WAF

Argomenti

- Perché migrare a AWS WAF?
- Come funziona la migrazione
- Avvertenze e limitazioni sulla migrazione
- Migrazione di un ACL Web da Classic a AWS WAFAWS WAF

Perché migrare a AWS WAF?

L'ultima versione di AWS WAF offre molti miglioramenti rispetto alla versione precedente, pur mantenendo la maggior parte dei concetti e della terminologia a cui siete abituati.

Nell'elenco seguente vengono descritte le principali modifiche apportate alla versione più recente di AWS WAF. Prima di continuare con la migrazione, dedica del tempo alla revisione di questo elenco e alla lettura del resto della guida. AWS WAF

- AWS Managed Rules per AWS WAF: i gruppi di regole ora disponibili tramite AWS Managed Rules forniscono protezione contro le minacce web più comuni. La maggior parte di questi gruppi di regole è inclusa gratuitamente in AWS WAF. Per ulteriori informazioni, vedi AWS Elenco dei gruppi di regole di Managed Rules e il post sul blog Announcing AWS Managed Rules for AWS WAF.
- Nuova AWS WAF API: la nuova API consente di configurare tutte le AWS WAF risorse utilizzando un unico set di API. Per distinguere tra applicazioni regionali e globali, la nuova API include un'impostazione `scope`. Per ulteriori informazioni sull'API, consulta le azioni WAFV2 e AWS i tipi di dati AWS WAFV2.

  Nelle API, negli SDK, nelle CLI e AWS CloudFormation, AWS WAF Classic mantiene i propri schemi di denominazione e a quest'ultima versione di AWS WAF si fa riferimento con un'aggiunta o, a seconda del contesto. `V2` `v2`
- Quote (limiti) di servizio semplificate: AWS WAF ora consente più regole per ACL Web e consente di esprimere modelli regex più lunghi. Per ulteriori informazioni, consulta AWS WAF quote.
- I limiti Web ACL ora si basano sulle esigenze di elaborazione: i limiti Web ACL sono ora basati sulle unità di capacità Web ACL (WCU). AWS WAF calcola la WCU per una regola in base alla capacità operativa richiesta per eseguirla. La WCU di una ACL Web è la somma della WCU di tutte le regole e i gruppi di regole dell'ACL Web.

  Per informazioni generali su WCU, vedere. Come AWS WAF funziona Per informazioni sull'utilizzo della WCU di ciascuna regola, vedere. Nozioni di base sulla dichiarazione delle regole
- Scrittura di regole basata su documenti: ora puoi scrivere ed esprimere regole, gruppi di regole e ACL Web in formato JSON. Non è più necessario utilizzare singole chiamate API per creare condizioni diverse e quindi associarle a una regola. Questo semplifica notevolmente il modo in cui si scrive e si gestisce il codice. È possibile accedere a un formato JSON delle ACL Web tramite la console quando si visualizza l'ACL Web, scegliendo Scarica ACL Web come JSON. Quando si crea una regola personalizzata, è possibile accedere alla relativa rappresentazione JSON scegliendo l'Editor di regole JSON.

- Nidificazione delle regole e supporto completo delle operazioni logiche: è possibile scrivere regole combinate complesse utilizzando istruzioni di regole logiche e utilizzando la nidificazione. È possibile creare istruzioni quali `[A AND NOT(B OR C)]`. Per ulteriori informazioni, consulta Dichiarazioni di regole logiche.
- Regole basate sulla frequenza migliorate: nell'ultima versione di AWS WAF, è possibile personalizzare la finestra temporale valutata dalla regola e il modo in cui la regola aggrega le richieste. È possibile personalizzare l'aggregazione utilizzando combinazioni di diverse caratteristiche delle richieste Web. Inoltre, le più recenti regole basate sulle tariffe reagiscono più rapidamente alle variazioni del traffico. Per ulteriori informazioni, consulta Istruzione regola basata sulla frequenza.
- Supporto dell'intervallo CIDR variabile per i set IP: le specifiche dei set IP ora offrono una maggiore flessibilità negli intervalli IP. Per IPv4, AWS WAF supporta. `/1` `/32` Per IPv6, supporta. AWS WAF `/1` `/128` Per ulteriori informazioni sui set di IP, consulta Istruzione regola di corrispondenza set di IP.
- Trasformazioni di testo concatenabili: AWS WAF può eseguire più trasformazioni di testo sul contenuto delle richieste Web prima di esaminarlo. Per ulteriori informazioni, consulta Trasformazioni di testo.
- Esperienza di console migliorata: la nuova AWS WAF console presenta un generatore di regole visive e un design della console più intuitivo per l'utente.
- Opzioni estese per AWS WAF le politiche di Firewall Manager: nella gestione degli ACL AWS WAF Web di Firewall Manager, è ora possibile creare un set di gruppi di regole che AWS WAF elaborano per primi e un set di gruppi di regole che AWS WAF elaborano per ultimi. Dopo aver applicato la AWS WAF policy, i proprietari di account locali possono aggiungere i propri gruppi di regole che AWS WAF elaborano tra questi due set. Per ulteriori informazioni sulle AWS WAF politiche di Firewall Manager, vedereAWS WAF politiche.
- AWS CloudFormation supporto per tutti i tipi di istruzioni delle regole: AWS WAF in AWS CloudFormation supporta tutti i tipi di istruzioni delle regole supportati dalla AWS WAF console e dall'API. Inoltre, è possibile convertire facilmente le regole che si scrivono in formato JSON nel formato YAML.

Come funziona la migrazione

La migrazione automatizzata trasferisce la maggior parte della configurazione ACL web AWS WAF classica, lasciando alcune cose che devi gestire manualmente.

Di seguito sono elencate le fasi di alto livello per la migrazione di un'ACL Web.

1. La migrazione automatizzata legge tutto ciò che riguarda l'ACL web esistente, senza modificare o eliminare nulla in Classic. AWS WAF Crea una rappresentazione dell'ACL web e delle relative risorse, compatibile con. AWS WAF Genera un AWS CloudFormation modello per il nuovo ACL Web e lo archivia in un bucket Amazon S3.
2. Il modello viene distribuito in AWS CloudFormation, al fine di ricreare l'ACL Web e le risorse correlate in. AWS WAF
3. Esaminare l'ACL Web e completare manualmente la migrazione, assicurandosi che la nuova ACL Web sfrutti appieno le funzionalità della versione più recente AWS WAF.
4. È possibile passare manualmente le risorse protette alla nuova ACL Web.

Avvertenze e limitazioni sulla migrazione

La migrazione non trasferisce tutte le tue impostazioni, esattamente come le hai in AWS WAF Classic. Alcuni elementi, come le regole gestite, non vengono mappate esattamente tra le due versioni. Altre impostazioni, come le associazioni dell'ACL Web con AWS le risorse protette, sono inizialmente disattivate nella nuova versione, quindi puoi aggiungerle quando sei pronto.

Nell'elenco seguente vengono descritte le avvertenze relative alla migrazione e vengono descritte tutti le fasi che è possibile eseguire in risposta. Utilizzare questa panoramica per pianificare la migrazione. Le fasi dettagliate della migrazione, più avanti, illustrano le fasi di mitigazione consigliate.

- Account singolo: puoi migrare solo le risorse AWS WAF Classic di qualsiasi account verso AWS WAF risorse per lo stesso account.
- Regole gestite: la migrazione non comporta alcuna regola gestita dai Marketplace AWS venditori. Alcuni Marketplace AWS venditori dispongono di regole gestite equivalenti a AWS WAF cui puoi abbonarti nuovamente. Prima di farlo, consulta le regole AWS gestite fornite con l'ultima versione di AWS WAF. La maggior parte di queste sono gratuite per AWS WAF gli utenti. Per informazioni sulle regole gestite, consulta Gruppi di regole gestite.
- Associazioni ACL Web: la migrazione non comporta alcuna associazione tra l'ACL Web e le risorse protette. Questa è un'impostazione di progettazione, per evitare di influire sul carico di lavoro di produzione. Dopo aver verificato che tutti gli elementi sono stati migrati correttamente, associare la nuova ACL Web alle risorse.

- Registrazione: la registrazione per l'ACL Web migrato è disabilitata per impostazione predefinita. Si tratta di un'impostazione predefinita. Abilita la registrazione quando sei pronto per passare dalla versione Classic a. AWS WAF AWS WAF
- AWS Firewall Manager gruppi di regole: la migrazione non gestisce i gruppi di regole gestiti da Firewall Manager. È possibile migrare un ACL Web gestito da Firewall Manager, ma la migrazione non include il gruppo di regole. Invece di utilizzare lo strumento di migrazione per questi ACL Web, ricrea la policy per il nuovo AWS WAF in Firewall Manager.

  > **Note**
  >
  > I gruppi di regole gestiti da Firewall Manager per AWS WAF Classic erano gruppi di regole di Firewall Manager. Con la nuova versione di AWS WAF, i gruppi di regole sono gruppi di AWS WAF regole. Dal punto di vista funzionale, sono la stessa cosa.

- AWS WAF Automazioni di sicurezza: non tentate di migrare alcuna automazione di AWS WAF sicurezza. La migrazione non converte le funzioni Lambda, che potrebbero essere utilizzate dalle automazioni. Quando è disponibile una nuova soluzione AWS WAF di Security Automations compatibile con la più recente AWS WAF, ridistribuisci quella soluzione.

Migrazione di un ACL Web da Classic a AWS WAFAWS WAF

Per eseguire la migrazione di un'ACL Web e passare ad essa, eseguire la migrazione automatica, quindi completare una serie di fasi manuali.

Argomenti

- Migrazione di un'ACL Web: migrazione automatizzata
- Migrazione di un'ACL Web: follow-up manuale
- Migrazione di un'ACL Web: ulteriori considerazioni
- Migrazione di un'ACL Web: passaggio

Migrazione di un'ACL Web: migrazione automatizzata

Per migrare automaticamente una configurazione ACL Web da Classic a AWS WAFAWS WAF

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

2. Scegli Passa alla AWS WAF versione classica e rivedi le impostazioni di configurazione per l'ACL web. Prendere nota delle impostazioni, considerando le avvertenze e le limitazioni descritte nella sezione precedente Avvertenze e limitazioni sulla migrazione.
3. Nel dialogo informativo in alto, individua la frase che inizia con Migrate web ACLs e scegli il collegamento alla procedura guidata di migrazione. Verrà lanciata la procedura guidata per la migrazione.

   Se non vedi la finestra di dialogo informativa, potresti averla chiusa dopo l'avvio della console Classic. AWS WAF Nella barra di navigazione, scegli Passa a nuovo, AWS WAF quindi scegli Passa alla AWS WAF versione classica e la finestra di dialogo informativa dovrebbe riapparire.
4. Selezionare l'ACL Web di cui si desidera eseguire la migrazione.
5. Per la configurazione della migrazione, fornisci un bucket Amazon S3 da utilizzare per il modello. È necessario un bucket Amazon S3 configurato correttamente per l'API di migrazione, per archiviare il AWS CloudFormation modello che genera.

   - Se il bucket è crittografato, la crittografia deve utilizzare chiavi Amazon S3 (SSE-S3). La migrazione non supporta la crittografia con AWS Key Management Service chiavi (SSE-KMS).
   - Il nome del bucket deve iniziare con `aws-waf-migration-`. Ad esempio, `aws-waf-migration-my-web-acl`.
   - Il bucket deve trovarsi nella regione in cui si sta distribuendo il modello. Ad esempio, per un accesso ACL Web`us-west-2`, è necessario utilizzare un bucket `us-west-2` in Amazon S3 e distribuire lo stack di modelli su. `us-west-2`
6. Per Policy del bucket S3, si consiglia di scegliere Applica automaticamente la policy del bucket richiesta per la migrazione. In alternativa, se si desidera gestire autonomamente il bucket, è necessario applicare manualmente le seguenti policy del bucket:

   - Per CloudFront le applicazioni Amazon globali (`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>/
*"
        }
    ]
}
```

- Per le applicazioni regionali Amazon API Gateway o Application Load Balancer ()`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. Per Scegliere come gestire le regole di cui non è possibile eseguire la migrazione, scegliere se escludere le regole di cui non è possibile eseguire la migrazione o interrompere la migrazione. Per informazioni sulle regole di cui non è possibile eseguire la migrazione, consulta Avvertenze e limitazioni sulla migrazione.
8. Seleziona Successivo.
9. Per Crea AWS CloudFormation modello, verifica le impostazioni, quindi scegli Inizia a creare AWS CloudFormation modello per iniziare il processo di migrazione. Questa operazione può richiedere alcuni minuti, a seconda della complessità dell'ACL Web.
10. In Crea ed esegui AWS CloudFormation stack per completare la migrazione, puoi scegliere di accedere alla AWS CloudFormation console per creare uno stack dal modello, per creare il nuovo ACL web e le relative risorse. Per fare ciò, scegli Create stack. AWS CloudFormation

Al termine del processo di migrazione automatica, è possibile procedere alle fasi di follow-up manuale. Per informazioni, consulta Migrazione di un'ACL Web: follow-up manuale.

Migrazione di un'ACL Web: follow-up manuale

Al termine della migrazione automatica, esaminare l'ACL Web appena creata e inserire i componenti che la migrazione non trasferisce. La procedura seguente illustra gli aspetti della gestione delle ACL Web che la migrazione non gestisce. Per l'elenco, consulta Avvertenze e limitazioni sulla migrazione.

Per completare la migrazione di base: fasi manuali

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.
2. La console dovrebbe utilizzare automaticamente la versione più recente di AWS WAF. Per verificarlo, nel riquadro di navigazione, verifica che sia possibile visualizzare l'opzione Passa alla AWS WAF versione classica. Se vedi Passa alla versione nuova AWS WAF, scegli questa opzione per passare alla versione più recente.
3. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).
4. Nella pagina ACL Web individuare la nuova ACL Web nell'elenco della regione in cui è stata creata. Scegliere il nome dell'ACL Web per visualizzare le relative impostazioni.
5. Controlla tutte le impostazioni per il nuovo ACL web confrontandole con l'ACL web AWS WAF classico precedente. Per impostazione predefinita, la registrazione e le associazioni di risorse protette sono disattivate. Puoi attivarle quando sei pronto al passaggio.
6. Se l'ACL web AWS WAF classico aveva una regola basata sulla tariffa con una condizione, tale condizione non è stata inserita nella migrazione. È possibile aggiungere condizioni alla regola nella nuova ACL Web.

   a. Nella pagina delle impostazioni ACL Web, scegliere la scheda Regole.

   b. Individua la regola basata sulla frequenza nell'elenco, selezionala e scegli Modifica.

   c. In Criteri per conteggiare la richiesta rispetto al limite di frequenza, selezionare Considera solo le richieste che corrispondono ai criteri in un'istruzione di regola, quindi fornire i criteri aggiuntivi. È possibile aggiungere i criteri utilizzando qualsiasi istruzione di regola nidificata, incluse le istruzioni logiche. Per informazioni sulle scelte effettuate, consulta Istruzione regola basata sulla frequenza.
7. Se l'ACL web AWS WAF classico aveva un gruppo di regole gestito, l'inclusione del gruppo di regole non è stata inclusa nella migrazione. È possibile aggiungere gruppi di regole gestite alla nuova ACL Web. Consulta le informazioni sui gruppi di regole gestite, incluso l'elenco delle regole AWS gestite disponibili con la nuova versione di AWS WAF, all'indirizzoGruppi di regole gestite. Per aggiungere un gruppo di regole gestite, effettuare le seguenti operazioni:

a. Nella pagina delle impostazioni ACL Web, scegliere la scheda Regole dell'ACL Web.

b. Scegliere Aggiungi regole, quindi Aggiungi gruppi di regole gestite.

c. Espandere l'elenco per il fornitore scelto e selezionare i gruppi di regole che si desidera aggiungere. Per Marketplace AWS i venditori, potresti dover sottoscrivere i gruppi di regole. Per ulteriori informazioni sull'utilizzo di gruppi di regole gestite nell'ACL Web, consulta Gruppi di regole gestite e Valutazione delle regole ACL Web e dei gruppi di regole.

Al termine del processo di migrazione di base, si consiglia di esaminare le proprie esigenze e di considerare ulteriori opzioni, per assicurarsi che la nuova configurazione sia il più efficiente possibile e che utilizzi le opzioni di sicurezza più recenti disponibili. Per informazioni, consulta Migrazione di un'ACL Web: ulteriori considerazioni.

Migrazione di un'ACL Web: ulteriori considerazioni

Esamina il tuo nuovo ACL web e considera le opzioni disponibili nel nuovo AWS WAF per assicurarti che la configurazione sia il più efficiente possibile e che utilizzi le ultime opzioni di sicurezza disponibili.

Regole AWS gestite aggiuntive

Prendi in considerazione l'implementazione di regole AWS gestite aggiuntive nell'ACL Web per aumentare il livello di sicurezza dell'applicazione. Queste sono incluse senza AWS WAF costi aggiuntivi. AWS Le Managed Rules includono i seguenti tipi di gruppi di regole:

- I gruppi di regole di base forniscono una protezione generale contro una serie di minacce comuni, ad esempio impedire l'inserimento di input non validi noti nell'applicazione e impedire l'accesso alla pagina di amministrazione.
- I gruppi di regole specifici dei casi d'uso forniscono una protezione incrementale per molti casi d'uso e ambienti diversi.
- Gli elenchi di reputazione IP forniscono informazioni di intelligence in base all'IP di origine del client.

Per ulteriori informazioni, consulta AWS Regole gestite per AWS WAF.

Ottimizzazione e pulizia delle regole

Riesamina le vecchie regole e considera l'ottimizzazione riscrivendole o rimuovendo quelle obsolete. Ad esempio, se in passato avete distribuito un AWS CloudFormation modello tratto dal paper tecnico sulle 10 principali vulnerabilità delle applicazioni Web OWASP, Prepare for the OWASP Top 10 Vulnerabilities Vulnerabilities Using AWS WAF e dal nostro nuovo white paper, dovreste prendere in considerazione la possibilità di sostituirlo con Managed Rules. AWS Sebbene il concetto contenuto nel documento sia ancora applicabile e possa aiutarti a scrivere le tue regole, le regole create dal modello sono state ampiamente sostituite dalle Managed Rules. AWS

Parametri e CloudWatch allarmi di Amazon

Rivedi i CloudWatch parametri di Amazon e configura gli allarmi secondo necessità. La migrazione non trasferisce gli CloudWatch allarmi ed è possibile che i nomi delle metriche non siano quelli che desideri.

Riesame con il team delle applicazioni

Collabora con il team delle applicazioni e controlla l'assetto di sicurezza. Scopri quali campi vengono analizzati frequentemente dall'applicazione e aggiungi regole per sanificare l'input di conseguenza. Verifica la presenza di eventuali casi limite e aggiungi regole per rilevare questi casi se la logica di business dell'applicazione non riesce a elaborarli.

Pianificare il passaggio

Pianificare la tempistica del passaggio con il team delle applicazioni. Il passaggio dalla vecchia associazione Web ACL a quella nuova può richiedere un po' di tempo per propagarsi in tutte le aree in cui sono archiviate le risorse. Il tempo di propagazione può variare da pochi secondi a diversi minuti. Durante questo periodo, alcune richieste verranno elaborate dal vecchio ACL Web e altre dal nuovo ACL Web. Le tue risorse saranno protette in tutto lo switch, ma potresti notare delle incongruenze nella gestione delle richieste mentre lo switch è in corso.

Quando si è pronti per il passaggio, seguire la procedura in Migrazione di un'ACL Web: passaggio.

Migrazione di un'ACL Web: passaggio

Dopo aver verificato le nuove impostazioni ACL web, puoi iniziare a utilizzarle al posto dell'ACL web AWS WAF classico.

Per iniziare a utilizzare il nuovo ACL web AWS WAF

1. Associa l'ACL AWS WAF Web alle risorse che desideri proteggere, seguendo le indicazioni disponibili all'indirizzo. Associazione o dissociazione di un ACL Web con una risorsa AWS Ciò annulla automaticamente l'associazione delle risorse dalla vecchia ACL Web.

   La propagazione dello switch può richiedere da alcuni secondi a diversi minuti. Durante questo periodo, alcune richieste potrebbero essere elaborate dal vecchio ACL Web e altre dal nuovo ACL Web. Le tue risorse saranno protette in tutto lo switch, ma potresti notare incongruenze nella gestione delle richieste fino al completamento.
2. Configurare la registrazione per la nuova ACL Web seguendo le linee guida riportate in Registrazione del traffico AWS WAF ACL Web.
3. (Facoltativo) Se l'ACL web AWS WAF classico non è più associato a nessuna risorsa, valuta la possibilità di rimuoverlo completamente da Classic. AWS WAF Per informazioni, consulta Eliminazione di un'ACL Web.

AWS WAF Classico

> **Note**
>
> Questa è la documentazione di Classic AWS WAF . Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

AWS WAF Classic è un firewall per applicazioni Web che consente di monitorare le richieste HTTP e HTTPS inoltrate a un'API Amazon API Gateway, Amazon CloudFront o un Application Load Balancer. AWS WAF Classic ti consente anche di controllare l'accesso ai tuoi contenuti. In base a condizioni specificate, ad esempio gli indirizzi IP da cui provengono le richieste o i valori delle stringhe di query, API Gateway CloudFront o Application Load Balancer risponde alle richieste con il contenuto richiesto o con un codice di stato HTTP 403 (Forbidden). È inoltre possibile configurare la restituzione CloudFront di una pagina di errore personalizzata quando una richiesta viene bloccata.

Argomenti

Configurazione AWS WAF Classic

> **Note**
>
> Questa è la documentazione di AWS WAF Classic. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Questo argomento descrive i passaggi preliminari, come la creazione di un account utente, per prepararti all'uso di AWS WAF Classic. Non ti viene addebitato alcun costo per questi. Ti vengono addebitati solo i AWS servizi che utilizzi.

> **Note**
>
> Se sei un nuovo utente AWS WAF, non seguire questi passaggi di configurazione per AWS WAF Classic. Segui invece i passaggi per la versione più recente di AWS WAF, all'indirizzoConfigurazione.

Dopo aver completato questi passaggi, vedi Guida introduttiva a AWS WAF Classic per continuare a usare AWS WAF Classic.

> **Note**
>
> AWS Shield Standard è incluso in AWS WAF Classic e non richiede configurazioni aggiuntive. Per ulteriori informazioni, consulta Come funzionano AWS Shield e Shield Advanced.

Prima di utilizzare AWS WAF Classic o AWS Shield Advanced per la prima volta, completa i passaggi in questa sezione.

Argomenti

- Iscriviti per un Account AWS

- Creazione di un utente amministratore
- Download degli strumenti

Iscriviti per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Creazione di un utente amministratore

Dopo la registrazione Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Creazione di un utente amministratore

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .

2. In Centro identità AWS IAM, assegna l'accesso amministrativo a un utente amministrativo.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Download degli strumenti

AWS Management Console Include una console per AWS WAF Classic, ma se desideri accedere a AWS WAF Classic a livello di codice, consulta quanto segue:

- Se desideri chiamare l'API AWS WAF Classic senza dover gestire dettagli di basso livello come l'assemblaggio di richieste HTTP non elaborate, puoi utilizzare un SDK. AWS Gli AWS SDK forniscono funzioni e tipi di dati che racchiudono le funzionalità di Classic e di altri servizi. AWS WAF AWS Per scaricare un AWS SDK, consulta la pagina relativa, che include anche i prerequisiti e le istruzioni di installazione:
  - Java
  - JavaScript
  - .NET

- Node.js
- PHP
- Python
- Ruby

Per un elenco completo degli AWS SDK, consulta Tools for Amazon Web Services.

- Se utilizzi un linguaggio di programmazione che AWS non fornisce un SDK, l'AWS WAF API Reference documenta le operazioni supportate da AWS WAF Classic.
- Il AWS Command Line Interface (AWS CLI) supporta AWS WAF Classic. Ti AWS CLI consente di controllare più AWS servizi dalla riga di comando e di automatizzarli tramite script. Per ulteriori informazioni, consulta AWS Command Line Interface.
- AWS Tools for Windows PowerShell supporta Classic AWS WAF . Per ulteriori informazioni, consulta la Documentazione di riferimento per Cmdlet AWS Tools for PowerShell.

Come funziona AWS WAF Classic

> **Note**
>
> Questa è la documentazione di AWS WAF Classic. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Utilizzi AWS WAF Classic per controllare il modo in cui API Gateway, Amazon CloudFront o un Application Load Balancer rispondono alle richieste web. Inizi creando condizioni, regole e liste di controllo accessi Web (ACL Web) Definisci le condizioni, combini le condizioni in regole e combini le regole in un'ACL Web.

> **Note**
>
> Puoi anche usare AWS WAF Classic per proteggere le tue applicazioni ospitate nei contenitori Amazon Elastic Container Service (Amazon ECS). Amazon ECS è un servizio di gestione dei container veloce e altamente scalabile che semplifica l'esecuzione, l'arresto e la gestione dei contenitori Docker su un cluster. Per utilizzare questa opzione, configuri

Amazon ECS per utilizzare un Application Load Balancer con funzionalità AWS WAF Classic per instradare e proteggere il traffico HTTP/HTTPS (livello 7) tra le attività del tuo servizio. Per ulteriori informazioni, consulta l'argomento Service Load Balancing nella Amazon Elastic Container Service Developer Guide.

Condizioni

Le condizioni definiscono le caratteristiche di base che vuoi che AWS WAF Classic tenga in considerazione nelle richieste web:

- Gli script che potrebbero essere dannosi. Alcuni malintenzionati incorporano script che possono sfruttare le vulnerabilità nelle applicazioni Web. Questa operazione è nota come Cross-site scripting.
- Gli indirizzi IP o gli intervalli di indirizzi di origine delle richieste.
- Il paese o la posizione geografica di origine delle richieste.
- La lunghezza delle parti specificate della richiesta, ad esempio la stringa di query.
- Il codice SQL che potrebbe essere dannoso. I malintenzionati provano a estrarre i dati dal tuo database incorporando codice SQL dannoso in una richiesta Web. Questa operazione è nota come SQL injection.
- Le stringhe presenti nella richiesta, ad esempio, i valori nell'intestazione `User-Agent` o le stringhe di testo visualizzate nella stringa di query. È inoltre possibile usare espressioni regolari (regex) per specificare queste stringhe.

Alcune condizioni richiedono più valori. Ad esempio, è possibile specificare fino a 10.000 indirizzi IP o intervalli di indirizzi IP in una condizione IP.

Regolamento

Combini le condizioni in regole per indirizzare con precisione le richieste che desideri consentire, bloccare o contare. AWS WAF Classic offre due tipi di regole:

Regola normale

Le regole normali usano solo le condizioni per indirizzare richieste specifiche. Ad esempio, in base alle richieste recenti che hai ricevuto da un malintenzionato, potresti creare una regola che includa le seguenti condizioni:

- Le richieste provengono da 192.0.2.44.

- Contengono il valore `BadBot` nell'intestazione `User-Agent`.
- Sembrano includere codice di tipo SQL nella stringa di query.

Quando una regola include più condizioni, come in questo esempio, AWS WAF Classic cerca le richieste che soddisfano tutte le condizioni, ovvero le condizioni `AND` insieme.

Aggiungere almeno una condizione per un regola normale. Una regola normale senza condizioni non può corrispondere ad alcuna richiesta, pertanto l'operazione della regola (consenso, conteggio o blocco) non viene mai attivata.

Regola basata sulla frequenza

Le regole basate sulla frequenza sono come le regole normali con un limite di frequenza aggiunto. Una regola basata sulla frequenza conta le richieste che arrivano da indirizzi IP che soddisfano le condizioni della regola. Se le richieste provenienti da un indirizzo IP superano il limite di frequenza in un periodo di cinque minuti, la regola può attivare un'operazione. L'attivazione dell'azione può richiedere uno o due minuti.

Le condizioni sono facoltative per le regole basate sulla frequenza. Se non aggiungi alcuna condizione in una regola basata sulla frequenza, il limite di frequenza si applica a tutti gli indirizzi IP. Se combini le condizioni con il limite di frequenza, il limite di frequenza si applica a indirizzi IP che soddisfano le condizioni.

Ad esempio, in base alle richieste recenti che hai ricevuto da un malintenzionato, potresti creare una regola basata sulla frequenza che includa le seguenti condizioni:

- Le richieste provengono da 192.0.2.44.
- Contengono il valore `BadBot` nell'intestazione `User-Agent`.

In questa regola basata sulla frequenza, definisci anche un limite di velocità. In questo esempio, supponiamo di creare un limite di frequenza di 1.000. Le richieste che soddisfano entrambe le condizioni precedenti e superano le 1.000 richieste per cinque minuti attivano l'operazione della regola (blocco o conteggio), definita nell'ACL Web.

Le richieste che non soddisfano entrambe le condizioni non vengono conteggiate ai fini del limite di frequenza e non sono influenzate da questa regola.

Come secondo esempio, supponiamo che desideri limitare le richieste a una determinata pagina nel sito Web. Per farlo, è possibile aggiungere la seguente condizione di corrispondenza stringa a una regola basata sulla frequenza:

- Il valore Part of the request to filter on (Parte della richiesta sulla quale filtrare) è `URI`.
- Il valore Match Type (Tipo di corrispondenza) è `Starts with`.
- Il valore Value to match (Valore per la corrispondenza) è `login`.

Inoltre, è necessario specificare un `RateLimit` di 1.000.

Tramite l'aggiunta di questa regola basata sulla frequenza all'ACL Web, è possibile limitare le richieste alla pagina di accesso senza influenzare il resto del sito.

ACL Web

Dopo aver combinato le condizioni in regole, le regole vengono combinate in un'ACL Web. Qui puoi definire un'azione per ogni regola (consenti, blocca o conta) e un'azione predefinita:

Un'operazione per ogni regola

Quando una richiesta Web soddisfa tutte le condizioni di una regola, AWS WAF Classic può bloccare la richiesta o consentire l'inoltro della richiesta all'API Gateway API, alla CloudFront distribuzione o a un Application Load Balancer. Specificate l'azione che desiderate che AWS WAF Classic esegua per ogni regola.

AWS WAF Classic confronta una richiesta con le regole di un ACL Web nell'ordine in cui sono elencate le regole. AWS WAF Classic esegue quindi l'azione associata alla prima regola a cui corrisponde la richiesta. Ad esempio, se una richiesta Web soddisfa una regola che consente le richieste e un'altra regola che blocca le richieste, AWS WAF Classic consentirà o bloccherà la richiesta a seconda della regola elencata per prima.

Se desideri testare una nuova regola prima di iniziare a utilizzarla, puoi anche configurare AWS WAF Classic per contare le richieste che soddisfano tutte le condizioni della regola. Come per le regole che consentono o bloccano le richieste, una regola che conta le richieste è influenzata dalla sua posizione nell'elenco delle regole nell'ACL Web. Ad esempio, se una richiesta Web corrisponde a una regola che consente le richieste e un'altra regola che conteggia le richieste e se la regola che consente le richieste è elencata per prima, questa richiesta non viene conteggiata.

Operazione predefinita

L'azione predefinita determina se AWS WAF Classic consente o blocca una richiesta che non soddisfa tutte le condizioni di nessuna delle regole dell'ACL Web. Ad esempio, supponi di creare un'ACL Web e di aggiungere solo la regola che hai definito prima:

- Le richieste provengono da 192.0.2.44.
- Contengono il valore `BadBot` nell'intestazione `User-Agent`.
- Sembrano includere codice di tipo SQL dannoso nella stringa di query.

Se una richiesta non soddisfa tutte e tre le condizioni della regola e se l'azione predefinita è`ALLOW`, AWS WAF Classic inoltra la richiesta ad API Gateway CloudFront o a un Application Load Balancer e il servizio risponde con l'oggetto richiesto.

Se aggiungi due o più regole a un ACL web, AWS WAF Classic esegue l'azione predefinita solo se una richiesta non soddisfa tutte le condizioni di nessuna delle regole. Ad esempio, supponi di aggiungere una seconda regola che contenga una condizione:

- Le richieste che contengono il valore `BIGBadBot` nell'intestazione `User-Agent`.

AWS WAF Classic esegue l'azione predefinita solo quando una richiesta non soddisfa tutte e tre le condizioni della prima regola e non soddisfa una condizione della seconda regola.

In alcune occasioni, AWS WAF potrebbe verificarsi un errore interno che ritarda la risposta ad Amazon API Gateway, Amazon CloudFront o un Application Load Balancer sull'opportunità di consentire o bloccare una richiesta. In tali occasioni CloudFront generalmente consente la richiesta o fornisce il contenuto. API Gateway e Application Load Balancer in genere rifiutano la richiesta e non distribuiscono i contenuti.

AWS WAF Prezzi classici

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Con AWS WAF Classic, paghi solo per gli ACL Web e le regole che crei e per il numero di richieste HTTP esaminate da AWS WAF Classic. Per ulteriori informazioni, consulta la sezione Prezzi AWS WAF Classic.

Guida introduttiva a AWS WAF Classic

> **Note**
>
> Questa è la documentazione di AWS WAF Classic. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Questo tutorial mostra come utilizzare AWS WAF Classic per eseguire le seguenti attività:

- Configura AWS WAF Classic.
- Crea un elenco di controllo degli accessi Web (Web ACL) utilizzando la console AWS WAF Classic e specifica le condizioni che desideri utilizzare per filtrare le richieste Web. Ad esempio, è possibile specificare gli indirizzi IP da cui provengono le richieste e i valori nella richiesta che vengono utilizzati solo da aggressori.
- Aggiungere le condizioni a una regola. Il regolamento consente di indicare quali richieste Web bloccare e quali consentire. Una richiesta Web deve soddisfare tutte le condizioni di una regola prima che AWS WAF Classic blocchi o consenta le richieste in base alle condizioni specificate.
- Aggiungere il regolamento al proprio ACL Web. A questo punto, è necessario specificare se si desidera bloccare o consentire le richieste Web in base alle condizioni aggiunte per ogni regola.
- Specificare un'azione predefinita, bloccarla o consentirla. Questa è l'azione che AWS WAF Classic esegue quando una richiesta web non corrisponde a nessuna delle tue regole.
- Scegli la CloudFront distribuzione Amazon per cui desideri che AWS WAF Classic esamini le richieste web. Questo tutorial illustra solo i passaggi per CloudFront, ma il processo per le API Application Load Balancer e Amazon API Gateway è essenzialmente lo stesso. AWS WAF Classic for CloudFront è disponibile per tutti. Regioni AWS AWS WAF La versione classica da utilizzare con API Gateway o Application Load Balancer è disponibile nelle regioni elencate negli endpoint del AWS servizio.

> **Note**
>
> AWS in genere ti addebita meno di 0,25 USD al giorno per le risorse che crei durante questo tutorial. Una volta completato il tutorial, ti consigliamo di eliminare le risorse per evitare di incorrere in spese non necessarie.

Argomenti

Passaggio 1: configura Classic AWS WAF

Se non hai già seguito la procedura di configurazione generale riportata in precedenzaConfigurazione AWS WAF Classic, fallo ora.

Fase 2: creare un'ACL Web

La console AWS WAF Classic guida l'utente nel processo di configurazione di AWS WAF Classic per bloccare o consentire le richieste Web in base a condizioni specificate, ad esempio gli indirizzi IP da cui provengono le richieste o i valori nelle richieste. In questa fase verrà creata un'ACL Web.

Per creare un'ACL Web

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.

2. Se è la prima volta che usi la AWS WAF versione classica, scegli Vai alla AWS WAF versione classica, quindi scegli Configura Web ACL.

   Se hai già utilizzato la AWS WAF versione classica, scegli Web ACL nel riquadro di navigazione, quindi scegli Crea ACL web.

3. Nella pagina Name web ACL (Nomina l'ACL Web), inserire un nome per Web ACL name (Nome ACL Web).

   > **Note**
   >
   > Non è possibile modificare il nome dopo aver creato l'ACL Web.

4. Per il nome della CloudWatch metrica, inserisci un nome. Il nome può contenere solo caratteri alfanumerici (A - Z, a - z, 0 - 9). Non può contenere spazi.

   > **Note**
   >
   > Non è possibile modificare il nome dopo aver creato l'ACL Web.

5. In Region (Regione), scegliere una Regione. Se associerai questo ACL web a una CloudFront distribuzione, scegli Global () CloudFront.
6. Per la AWS risorsa da associare, scegliete la risorsa che desiderate associare al vostro ACL web, quindi scegliete Avanti.

Fase 3: creare una condizione di corrispondenza IP

Una condizione di corrispondenza IP specifica gli indirizzi IP o gli intervalli dell'indirizzo IP da cui ha origine la richiesta. In questa fase verrà creata una condizione di corrispondenza IP. In un secondo momento, sarà necessario specificare se si desidera consentire o bloccare le richieste provenienti da indirizzi IP specificati.

> **Note**
>
> Per ulteriori informazioni sulle condizioni di corrispondenza IP, consulta Utilizzo di condizioni di corrispondenza IP.

Per creare una condizione di corrispondenza IP

1. Nella pagina Create conditions (Crea condizioni), per IP match conditions (Condizioni di corrispondenza IP), scegliere Create condition (Crea condizione).
2. Nella finestra di dialogo Create IP match condition (Crea condizione di corrispondenza IP), per Name (Nome), immettere un nome. Il nome può contenere solo caratteri alfanumerici (A - Z, a - z, 0 - 9) o i seguenti caratteri speciali: _-!"#`+*},./ .
3. Per Address (Indirizzo), immettere 192.0.2.0/24. Questo intervallo dell'indirizzo IP specificato nella notazione CIDR include gli indirizzi IP da 192.0.2.0 a 192.0.2.255. (L'intervallo dell'indirizzo IP 192.0.2.0/24 è solo un esempio, perciò nessuna richiesta Web avrà origine da questi indirizzi IP).

   AWS WAF La versione classica supporta gli intervalli di indirizzi IPv4: /8 e qualsiasi intervallo compreso tra /16 e /32. AWS WAF Classic supporta gli intervalli di indirizzi IPv6: /24, /32, /48, /56, /64 e /128. Per specificare un solo indirizzo IP, ad esempio 192.0.2.44, immettere 192.0.2.44/32. Altri intervalli non sono supportati.

   Per ulteriori informazioni sulla notazione CIDR, consulta Supernetting su Wikipedia.
4. Scegli Crea.

Fase 4: creare una condizione di corrispondenza geografica

Una condizione di corrispondenza geografica specifica il paese o i paesi da cui hanno origine le richieste. In questa fase verrà creata una condizione di corrispondenza geografica. In un secondo momento, sarà necessario specificare se si desidera consentire o bloccare le richieste provenienti da paesi specificati.

> **Note**
>
> Per ulteriori informazioni sulle condizioni di corrispondenza geografica, consulta Utilizzo di condizioni di corrispondenza geografica.

Per creare una condizione di corrispondenza geografica

1. Nella pagina Create conditions (Crea condizioni), per Geo match conditions (Condizioni di corrispondenza geografica), scegliere Create condition (Crea condizione).

2. Nella finestra di dialogo Create geo match condition (Crea condizione di corrispondenza geografica), per Name (Nome), immettere un nome. Il nome può contenere solo caratteri alfanumerici (A - Z, a - z, 0 - 9) o i seguenti caratteri speciali: _-!"#`+*},./ .
3. Scegliere un Location type (Tipo di luogo) e un paese. Attualmente, Location type (Tipo di posizione) può essere solo Country (Paese).
4. Scegliere Add location (Aggiungi luogo).
5. Scegli Crea.

Fase 5: creare una condizione di corrispondenza stringa

Una condizione di corrispondenza delle stringhe identifica le stringhe che si desidera che AWS WAF Classic cerchi in una richiesta, ad esempio un valore specificato in un'intestazione o in una stringa di query. Di solito, una stringa è composta da caratteri ASCII stampabili, ma è possibile specificare qualsiasi carattere esadecimale da 0x00 a 0xFF (decimale da 0 a 255). In questa fase verrà creata una condizione di corrispondenza stringa. In un secondo momento, sarà necessario specificare se si desidera consentire o bloccare le richieste che contengono le stringhe specificate.

> **Note**
>
> Per ulteriori informazioni sulle condizioni di corrispondenza stringa, consulta Utilizzo di condizioni di corrispondenza per stringa.

Per creare una condizione di corrispondenza stringa

1. Nella pagina Create conditions (Crea condizioni), per String and regex match conditions (Condizioni di corrispondenza e regex stringa), scegliere Create condition (Crea condizione).
2. Nella finestra di dialogo Create string match condition (Crea condizione di corrispondenza stringa), immettere i seguenti valori:

   Nome

   Inserire un nome. Il nome può contenere solo caratteri alfanumerici (A - Z, a - z, 0 - 9) o i seguenti caratteri speciali: _-!"#`+*},./ .

   Type

   Scegliere String match (Corrispondenza stringa).

Parte della richiesta su cui applicare un filtro

Scegliete la parte della richiesta Web che desiderate che AWS WAF Classic esamini per una stringa specificata.

Per questo esempio, scegliere Header (Intestazione).

> **Note**
>
> Se scegliete Body come valore di Parte della richiesta su cui filtrare, AWS WAF Classic ispeziona solo i primi 8192 byte (8 KB) perché CloudFront inoltra solo i primi 8192 byte per l'ispezione. Per consentire o bloccare le richieste il cui corpo è più lungo di 8192 byte, puoi creare una condizione di vincolo di dimensione. (AWS WAF Classic ottiene la lunghezza del corpo dalle intestazioni della richiesta.) Per ulteriori informazioni, consulta Utilizzo di condizioni per i vincoli di dimensioni.

Intestazione (obbligatoria se la "Parte della richiesta su cui applicare un filtro" è "Intestazione")

Poiché hai scelto Intestazione come parte della richiesta su cui filtrare, devi specificare quale intestazione vuoi che AWS WAF Classic esamini. Immettere User-Agent. (Questo valore prevede la distinzione tra lettere maiuscole e minuscole).

Tipo di corrispondenza

Scegliere la posizione in cui deve comparire la stringa specificata nell'intestazione di User-Agent (Utente-Agente), ad esempio all'inizio, alla fine o in qualsiasi parte della stringa.

Per questo esempio, scegliete Exactly matches, il che indica che AWS WAF Classic esamina le richieste Web alla ricerca di un valore di intestazione identico al valore specificato.

Trasformazione

Nel tentativo di aggirare la AWS WAF versione classica, gli aggressori utilizzano una formattazione insolita nelle richieste Web, ad esempio aggiungendo spazi bianchi o codificando l'URL in parte o nella totalità della richiesta. Le trasformazioni convertono la richiesta Web in un formato più standard rimuovendo spazi, decodificando l'URL della richiesta oppure eseguendo altre operazioni in grado di eliminare gran parte delle formattazioni insolite, utilizzate comunemente dagli aggressori.

È possibile specificare solo un unico tipo di trasformazione del testo.

Per questo esempio, scegliere None (Nessuna).

Il valore è codificato con base64

Quando il valore inserito in Value to match (Valore per la corrispondenza) è già codificato con base64, selezionare questa casella di controllo.

Per questo esempio, non selezionare la casella di controllo.

Valore per la corrispondenza

Specificate il valore che desiderate che AWS WAF Classic cerchi nella parte delle richieste Web che avete indicato in Parte della richiesta su cui filtrare.

Per questo esempio, inserisci BadBot. AWS WAF Classic esaminerà il valore nell'`User-Agent`intestazione delle richieste Web. BadBot

La lunghezza massima di Value to match (Valore per la corrispondenza) è di 50 caratteri. Se si desidera specificare un valore con codifica base64, è possibile fornire fino a 50 caratteri prima della codifica.

3. Se desideri che AWS WAF Classic controlli le richieste Web alla ricerca di più valori, ad esempio un'`User-Agent`intestazione che contiene `BadBot` e una stringa di query che contiene`BadParameter`, hai due scelte:

   - Se si desidera consentire o bloccare le richieste Web solo quando contengono entrambi i valori (`AND`), è necessario creare una condizione di corrispondenza stringa per ogni valore.
   - Se si desidera consentire o bloccare le richieste Web solo quando contengono uno o entrambi i valori (`OR`), è necessario aggiungere entrambi i valori sulla stessa condizione di corrispondenza stringa.

   Per questo esempio, scegliere Create (Crea).

Fase 5A: creare una condizione di espressione regolare (facoltativo)

Una condizione di espressione regolare è un tipo di condizione di corrispondenza delle stringhe e simile in quanto identifica le stringhe che AWS WAF Classic deve cercare in una richiesta, ad esempio un valore specificato in un'intestazione o in una stringa di query. La differenza principale è che si utilizza un'espressione regolare (regex) per specificare il modello di stringa che si desidera che

AWS WAF Classic cerchi. In questa fase verrà creata una condizione di corrispondenza regex. In un secondo momento, sarà necessario specificare se si desidera consentire o bloccare le richieste che contengono le stringhe specificate.

> **Note**
>
> Per ulteriori informazioni sulle condizioni di corrispondenza regex, consulta Utilizzo di condizioni di corrispondenza per regex.

Per creare una condizione di corrispondenza regex

1. Nella pagina Create conditions (Crea condizioni), per String and regex match conditions (Condizioni di corrispondenza e regex stringa), scegliere Create condition (Crea condizione).
2. Nella finestra di dialogo Create string match condition (Crea condizione di corrispondenza stringa), immettere i seguenti valori:

   Nome

   Inserire un nome. Il nome può contenere solo caratteri alfanumerici (A - Z, a - z, 0 - 9) o i seguenti caratteri speciali: _-!"#`+*},./ .

   Type

   Scegliere Regex match (Corrispondenza regex).

   Parte della richiesta su cui applicare un filtro

   Scegliete la parte della richiesta Web che desiderate che AWS WAF Classic esamini per una stringa specificata.

   Per questo esempio, scegliere Body (Corpo).

   > **Note**
   >
   > Se scegliete Body come valore di Parte della richiesta su cui filtrare, AWS WAF Classic ispeziona solo i primi 8192 byte (8 KB) perché CloudFront inoltra solo i primi 8192 byte per l'ispezione. Per consentire o bloccare le richieste il cui corpo è più lungo di 8192 byte, puoi creare una condizione di vincolo di dimensione. (AWS WAF

Classic ottiene la lunghezza del corpo dalle intestazioni della richiesta.) Per ulteriori informazioni, consulta Utilizzo di condizioni per i vincoli di dimensioni.

Trasformazione

Nel tentativo di aggirare AWS WAF Classic, gli aggressori utilizzano una formattazione insolita nelle richieste web, ad esempio aggiungendo spazi bianchi o codificando gli URL in parte o nella totalità della richiesta. Le trasformazioni convertono la richiesta Web in un formato più standard rimuovendo spazi, decodificando l'URL della richiesta oppure eseguendo altre operazioni in grado di eliminare gran parte delle formattazioni insolite, utilizzate comunemente dagli aggressori.

È possibile specificare solo un unico tipo di trasformazione del testo.

Per questo esempio, scegliere None (Nessuna).

Modelli regex che soddisfano la richiesta

Scegliere Create regex pattern set (Crea set del modello regex).

Nuovo nome del set del modello

Immettete un nome e specificate lo schema regex che desiderate che Classic cerchi. AWS WAF

Immettete quindi l'espressione regolare I [a@] mAb [a@] DRequest. AWS WAF Classic esaminerà l'`User-Agent`intestazione delle richieste web per i valori:

- Io sono BadRequest
- IamAB@dRequest
- Io @mA BadRequest
- I@mAB@dRequest

3. Scegliere Create pattern set and add filter (Crea set del modello e aggiungi filtro).
4. Scegli Crea.

Fase 6: creare una condizione di corrispondenza SQL injection

Una condizione di SQL injection match identifica la parte delle richieste Web, ad esempio un'intestazione o una stringa di query, che si desidera che AWS WAF Classic esamini per rilevare

la presenza di codice SQL dannoso. Gli aggressori utilizzano query SQL per estrarre i dati dal database. In questa fase verrà creata una condizione di corrispondenza SQL injection. In un secondo momento, sarà necessario specificare se si desidera consentire o bloccare le richieste che sembrano contenere codice SQL dannoso.

> **Note**
>
> Per ulteriori informazioni sulle condizioni di corrispondenza stringa, consulta Utilizzo di condizioni di corrispondenza SQL injection.

Per creare condizione di corrispondenza SQL injection

1. Nella pagina Create conditions (Crea condizioni), per SQL injection conditions (Condizioni di corrispondenza SQL injection), scegliere Create condition (Crea condizione).
2. Nella finestra di dialogo Create SQL injection match condition (Crea condizione di corrispondenza SQL injection), immettere i seguenti valori:

   Nome

   Inserire un nome.

   Parte della richiesta su cui applicare un filtro

   Scegliete la parte delle richieste Web che AWS WAF Classic deve ispezionare per rilevare la presenza di codice SQL dannoso.

   Per questo esempio, scegliere Query string (Stringa di query).

   > **Note**
   >
   > Se scegli Body come valore di Parte della richiesta su cui filtrare, AWS WAF Classic ispeziona solo i primi 8192 byte (8 KB) perché CloudFront inoltra solo i primi 8192 byte per l'ispezione. Per consentire o bloccare le richieste il cui corpo è più lungo di 8192 byte, puoi creare una condizione di vincolo di dimensione. (AWS WAF Classic ottiene la lunghezza del corpo dalle intestazioni della richiesta.) Per ulteriori informazioni, consulta Utilizzo di condizioni per i vincoli di dimensioni.

Trasformazione

Per questo esempio, scegliere URL decode (decodifica URL).

Gli aggressori utilizzano una formattazione insolita, come la codifica degli URL, nel tentativo di aggirare la versione classica. AWS WAF L'opzione di decodifica dell'URL elimina parte di tale formattazione nella richiesta web prima che Classic esamini la richiesta. AWS WAF

È possibile specificare solo un unico tipo di trasformazione del testo.

3. Scegli Crea.
4. Seleziona Successivo.

Fase 7: (facoltativo) creare condizioni aggiuntive

AWS WAF Classic include altre condizioni, tra cui le seguenti:

- Condizioni relative ai vincoli di dimensione: identifica la parte delle richieste Web, ad esempio un'intestazione o una stringa di query, di cui si desidera che AWS WAF Classic controlli la lunghezza. Per ulteriori informazioni, consulta Utilizzo di condizioni per i vincoli di dimensioni.
- Le condizioni di corrispondenza degli script tra siti: identifica la parte delle richieste Web, ad esempio un'intestazione o una stringa di query, che desideri esaminare per individuare eventuali script dannosi. AWS WAF Per ulteriori informazioni, consulta Utilizzo di condizioni di corrispondenza Cross-site scripting.

Se lo desideri, puoi creare tali condizioni ora o passare a Fase 8: creare una regola e aggiunta delle condizioni.

Fase 8: creare una regola e aggiunta delle condizioni

Crei una regola per specificare le condizioni che vuoi che AWS WAF Classic cerchi nelle richieste web. Se aggiungi più di una condizione a una regola, una richiesta Web deve soddisfare tutte le condizioni della regola affinché AWS WAF Classic consenta o blocchi le richieste basate su quella regola.

> **Note**
>
> Per ulteriori informazioni sulle regole, consulta Utilizzo delle regole.

Per creare una regola e aggiungere condizioni

1. Nella pagina Create rules (crea regolamento), scegliere Create rule (Crea regola).
2. Nella finestra di dialogo Create rule (Crea regola), immettere i seguenti valori:

   Nome

   Inserire un nome.

   CloudWatch nome della metrica

   Inserisci un nome per la CloudWatch metrica che AWS WAF Classic creerà e assocerà alla regola. Il nome può contenere solo caratteri alfanumerici (A - Z, a - z, 0 - 9). Non può contenere spazi.

   Tipo di regola

   Scegliere Regola regolare o regola basata sulla frequenza. Il regolamento basato sulla frequenza è identico agli altri regolamenti, ma prende in considerazione anche quante richieste arrivano dall'indirizzo IP in un periodo di cinque minuti. Per ulteriori informazioni sui tipi di regole, consulta Come funziona AWS WAF Classic. Per questo esempio, scegliere `Regular rule`.

   Limite frequenza

   Per una regola basata sulla frequenza, immetti il numero massimo di richieste da consentire in un periodo di cinque minuti da un indirizzo IP che soddisfa le condizioni della regola.
3. Per la prima condizione da aggiungere alla regola, specificare le impostazioni seguenti:

   - Scegli se desideri che AWS WAF Classic consenta o blocchi le richieste in base al fatto che una richiesta web corrisponda o meno alle impostazioni della condizione.

     Per questo esempio, scegliere does (consenti).
   - Scegliere il tipo di condizione da aggiungere alla regola: una condizione set di corrispondenza IP, una condizione set di corrispondenza stringa o una condizione set di corrispondenza SQL injection.

Per questo esempio, scegliere originate from IP addresses in (origina da indirizzi IP in).

- Scegliere la condizione da aggiungere alla regola.

  Per questo esempio, scegliere la condizione di corrispondenza IP creata nell'attività precedente.

4. Scegliere Aggiungi condizione.
5. Aggiungere la condizione di corrispondenza geografica creata in precedenza. Specifica i seguenti valori:
   - When a request does (Quando una richiesta la rispetta)
   - originate from a geographic location in (provengono da una posizione geografica in)
   - Scegliere la condizione di corrispondenza geografica.
6. Seleziona Add another condition (Aggiungi un'altra condizione).
7. Aggiungere la condizione di corrispondenza stringa creata in precedenza. Specifica i seguenti valori:
   - When a request does (Quando una richiesta la rispetta)
   - match at least one of the filters in the string match condition (soddisfa almeno uno dei filtri nella condizione di corrispondenza stringa)
   - Scegliere la condizione di corrispondenza stringa.
8. Scegliere Aggiungi condizione.
9. Aggiungere la condizione di corrispondenza SQL injection creata in precedenza. Specifica i seguenti valori:
   - When a request does (Quando una richiesta la rispetta)
   - match at least one of the filters in the SQL injection match condition (soddisfa almeno uno dei filtri nella condizione di corrispondenza SQL injection)
   - Scegliere la condizione di corrispondenza SQL injection.
10. Scegliere Aggiungi condizione.
11. Aggiungere la condizione di vincolo di dimensione creata in precedenza. Specifica i seguenti valori:
    - When a request does (Quando una richiesta la rispetta)

- match at least one of the filters in the size constraint condition (soddisfa almeno uno dei filtri nella condizione di vincolo di dimensione)
- Scegliere la condizione di vincolo di dimensione,

12. Se è stata creata un'altra condizione, ad esempio una condizione regex, aggiungerla come illustrato in precedenza.
13. Scegli Crea.
14. Per Default action (Operazione predefinita), scegliere Allow all requests that don't match any rules (Abilita tutte le richieste che non soddisfano nessun regolamento).
15. Scegliere Review and create (Rivedi e crea).

Fase 9: aggiungere la regola all'ACL Web

Quando si aggiunge la regola a un'ACL Web, è necessario specificare le impostazioni seguenti:

- L'azione che vuoi che AWS WAF Classic esegua sulle richieste web che soddisfano tutte le condizioni della regola: consentire, bloccare o contare le richieste.
- L'operazione predefinita per l'ACL Web. Questa è l'azione che vuoi che AWS WAF Classic esegua sulle richieste web che non soddisfano tutte le condizioni della regola: consentire o bloccare le richieste.

AWS WAF Classic inizia a bloccare le richieste CloudFront Web che soddisfano tutte le seguenti condizioni (e tutte le altre che potresti aver aggiunto):

- Il valore dell'intestazione di `User-Agent` è `BadBot`
- (Se è stata creata e aggiunta una condizione regex) Il valore `Body` è costituito da una delle quattro stringhe che soddisfano il modello `I[a@]mAB[a@]dRequest`
- Le richieste provenienti da indirizzi IP nell'intervallo 192.0.2.0 - 192.0.2.255
- Le richieste provenienti dal paese selezionato nella condizione di corrispondenza geografica
- Le richieste che sembrano includere codice SQL dannoso nella stringa di query.

AWS WAF Classic consente di rispondere CloudFront a tutte le richieste che non soddisfano tutte e tre queste condizioni.

Fase 10: eliminare le risorse

Il tutorial è stato completato con successo. Per evitare che sul tuo account vengano addebitati costi aggiuntivi per la AWS WAF versione Classic, devi ripulire gli oggetti AWS WAF Classic che hai creato. In alternativa, è possibile modificare la configurazione affinché soddisfi le richieste Web da consentire, bloccare e contare.

> **Note**
>
> AWS in genere ti addebita meno di 0,25 USD al giorno per le risorse che crei durante questo tutorial. Al termine, ti consigliamo di eliminare le risorse per evitare di incorrere in spese non necessarie.

Per eliminare gli oggetti per i quali Classic addebita un AWS WAF costo

1. Dissocia il tuo ACL web dalla tua CloudFront distribuzione:

   a. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

      Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.

   b. Scegli il nome dell'ACL web che desideri eliminare. Si apre una pagina con i dettagli dell'ACL Web nel riquadro a destra.

   c. Nel riquadro di destra, nella scheda Regole, vai alla sezione AWS Risorse che utilizzano questa sezione ACL web. Per la CloudFront distribuzione a cui hai associato l'ACL web, scegli la x nella colonna Tipo.

2. Rimuovere le condizioni dalla regola:

   a. Nel pannello di navigazione, scegli Regole.

   b. Scegliere la regola creata durante il tutorial.

   c. Scegliere Edit rule (Modifica regola).

   d. Scegliere la x a destra dell'intestazione di ogni condizione.

   e. Scegli Aggiorna.

3. Rimuovere la regola dall'ACL Web ed eliminare le ACL Web:

   a. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).

b. Scegli il nome dell'ACL web che hai creato durante il tutorial. Si apre una pagina con i dettagli dell'ACL Web nel riquadro a destra.

c. Nella scheda Rules (Regolamento), scegliere Edit web ACL (Modifica ACL Web).

d. Scegliere la x a destra dell'intestazione della regola.

e. Scegliere Actions (Operazioni), quindi scegliere Delete web ACL (Elimina ACL Web).

4. Elimina la regola:

a. Nel pannello di navigazione, scegli Regole.

b. Scegliere la regola creata durante il tutorial.

c. Scegli Elimina.

d. Nella finestra di dialogo Delete (Elimina), scegliere di nuovo Delete (Elimina) per confermare.

AWS WAF Classic non prevede alcun addebito per le condizioni, ma se desideri completare la pulizia, esegui la procedura seguente per rimuovere i filtri dalle condizioni ed eliminare le condizioni.

Per eliminare i filtri e le condizioni

1. Eliminare l'intervallo di indirizzi IP nella condizione di corrispondenza IP ed eliminare la condizione:

a. Nel pannello di navigazione della console AWS WAF Classic, scegli Indirizzi IP.

b. Scegliere la condizione di corrispondenza IP creata durante il tutorial.

c. Selezionare la casella di controllo aggiunta per l'intervallo di indirizzi IP.

d. Scegliere Delete IP address or range (Elimina indirizzo IP o intervallo).

e. Nel riquadro IP match conditions (Condizioni di corrispondenza IP) scegliere Delete (Elimina).

f. Nella finestra di dialogo Delete (Elimina), scegliere di nuovo Delete (Elimina) per confermare.

2. Eliminare il filtro nella condizione di corrispondenza SQL injection ed eliminare la condizione:

a. Nel riquadro di navigazione scegliere SQL injection.

b. Scegliere la condizione di corrispondenza SQL injection creata durante il tutorial.

c. Selezionare la casella di controllo aggiunta per il filtro.

d. Scegli Delete filter (Elimina filtro).

e. Nel riquadro SQL injection conditions (Condizioni di corrispondenza SQL injection) scegliere Delete (Elimina).

f. Nella finestra di dialogo Delete (Elimina), scegliere di nuovo Delete (Elimina) per confermare.

3. Eliminare il filtro nella condizione di corrispondenza stringa ed eliminare la condizione:

a. Nel riquadro di navigazione, scegliere String and regex matching (Stringa e regex corrispondenti).

b. Scegliere la condizione di corrispondenza stringa creata durante il tutorial.

c. Selezionare la casella di controllo aggiunta per il filtro.

d. Scegli Delete filter (Elimina filtro).

e. Nel riquadro String match conditions (Condizioni di corrispondenza stringa) scegliere Delete (Elimina).

f. Nella finestra di dialogo Delete (Elimina), scegliere di nuovo Delete (Elimina) per confermare.

4. Se presente, eliminare il filtro nella condizione di corrispondenza regex ed eliminare la condizione:

a. Nel riquadro di navigazione, scegliere String and regex matching (Stringa e regex corrispondenti).

b. Scegliere la condizione di corrispondenza regex creata durante il tutorial.

c. Selezionare la casella di controllo aggiunta per il filtro.

d. Scegli Delete filter (Elimina filtro).

e. Nel riquadro Regex match conditions (Condizioni di corrispondenza regex) scegliere Delete (Elimina).

f. Nella finestra di dialogo Delete (Elimina), scegliere di nuovo Delete (Elimina) per confermare.

5. Eliminare il filtro nella condizione di vincolo di dimensione ed eliminare la condizione:

a. Nel riquadro di navigazione, scegliere Size constraints (Vincoli di dimensione).

b. Scegliere la condizione di vincolo di dimensione creata durante il tutorial.

c. Selezionare la casella di controllo aggiunta per il filtro.

d. Scegli Delete filter (Elimina filtro).

e. Nel riquadro Size constraint conditions (Condizioni di vincolo di dimensione) scegliere Delete (Elimina).

f. Nella finestra di dialogo Delete (Elimina), scegliere di nuovo Delete (Elimina) per confermare.

Creazione e configurazione di una lista di controllo accessi Web (ACL)

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Un elenco di controllo degli accessi Web (Web ACL) ti offre un controllo dettagliato sulle richieste Web a cui rispondono l'API Amazon API Gateway, la CloudFront distribuzione Amazon o l'Application Load Balancer. È possibile consentire o bloccare i seguenti tipi di richieste:

- Richieste che hanno origine da un intervallo di indirizzi IP o un indirizzo IP
- Richieste che hanno origine da un paese specifico o da paesi specifici
- Richieste che contengono una stringa specificata o corrispondono a un modello di espressione regolare (regex) in una particolare parte di richieste
- Richieste che superano una lunghezza specificata
- Richieste che sembrano contenere codice SQL dannoso (noto come SQL injection)
- Richieste che sembrano contenere script dannosi (noto come Cross-site scripting)

È possibile anche testare qualsiasi combinazione di queste condizioni oppure bloccare o contare le richieste Web che non solo soddisfano i criteri specificati, ma che inoltre superano un determinato numero di richieste in un periodo di 5 minuti.

Per scegliere le richieste a cui desideri consentire l'accesso ai contenuti o che desideri bloccare, esegui le seguenti attività:

1. Scegli l'operazione predefinita, consenso o blocco, per le richieste Web che non corrispondono a nessuna delle condizioni specificate. Per ulteriori informazioni, consulta Decisione dell'operazione predefinita per un'ACL Web.
2. Specifica le condizioni in base alle quali desideri consentire o bloccare le richieste:
   - Per consentire o bloccare le richieste in base al fatto che le richieste sembrano contenere script dannosi, crea condizioni di corrispondenza Cross-site scripting. Per ulteriori informazioni, consulta Utilizzo di condizioni di corrispondenza Cross-site scripting.
   - Per consentire o bloccare le richieste in base a gli indirizzi IP da cui hanno origine, crea condizioni di corrispondenza IP. Per ulteriori informazioni, consulta Utilizzo di condizioni di corrispondenza IP.
   - Per consentire o bloccare le richieste in base al paese da cui hanno origine, crea condizioni di corrispondenza geografica. Per ulteriori informazioni, consulta Utilizzo di condizioni di corrispondenza geografica.
   - Per consentire o bloccare le richieste in base al fatto che le richieste superino una lunghezza specificata, crea condizioni per i vincoli di dimensioni. Per ulteriori informazioni, consulta Utilizzo di condizioni per i vincoli di dimensioni.
   - Per consentire o bloccare le richieste in base al fatto che le richieste sembrano contenere codice SQL dannoso, crea condizioni di corrispondenza SQL injection. Per ulteriori informazioni, consulta Utilizzo di condizioni di corrispondenza SQL injection.
   - Per consentire o bloccare le richieste in base alle stringhe visualizzate nelle richieste, crea condizioni di corrispondenza stringa. Per ulteriori informazioni, consulta Utilizzo di condizioni di corrispondenza per stringa.
   - Per consentire o bloccare le richieste in base al modello regex visualizzato nelle richieste, crea condizioni di corrispondenza per regex. Per ulteriori informazioni, consulta Utilizzo di condizioni di corrispondenza per regex.
3. Aggiungi le condizioni a una o più regole. Se aggiungi più di una condizione alla stessa regola, le richieste web devono soddisfare tutte le condizioni affinché AWS WAF Classic consenta o blocchi le richieste in base alla regola. Per ulteriori informazioni, consulta Utilizzo delle regole. Facoltativamente, puoi utilizzare una regola basata sulla frequenza anziché una regola normale per limitare il numero di richieste provenienti da qualsiasi indirizzo IP che soddisfa le condizioni.
4. Aggiungi le regole a un'ACL Web. Per ogni regola, specifica se desideri che AWS WAF Classic consenta o blocchi le richieste in base alle condizioni che hai aggiunto alla regola. Se aggiungi più di una regola a un ACL web, AWS WAF Classic valuta le regole nell'ordine in cui sono elencate nell'ACL web. Per ulteriori informazioni, consulta Utilizzo delle ACL Web.

Quando aggiungi una nuova regola o aggiorni le regole esistenti, può essere necessario fino a un minuto affinché tali modifiche vengano visualizzate e risultino attive tra le ACL Web e le risorse.

Argomenti

Utilizzo delle condizioni

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Le condizioni specificano quando desideri consentire o bloccare le richieste.

- Per consentire o bloccare le richieste in base al fatto che le richieste sembrano contenere script dannosi, crea condizioni di corrispondenza Cross-site scripting. Per ulteriori informazioni, consulta Utilizzo di condizioni di corrispondenza Cross-site scripting.
- Per consentire o bloccare le richieste in base a gli indirizzi IP da cui hanno origine, crea condizioni di corrispondenza IP. Per ulteriori informazioni, consulta Utilizzo di condizioni di corrispondenza IP.
- Per consentire o bloccare le richieste in base al paese da cui hanno origine, crea condizioni di corrispondenza geografica. Per ulteriori informazioni, consulta Utilizzo di condizioni di corrispondenza geografica.
- Per consentire o bloccare le richieste in base al fatto che le richieste superino una lunghezza specificata, crea condizioni per i vincoli di dimensioni. Per ulteriori informazioni, consulta Utilizzo di condizioni per i vincoli di dimensioni.

- Per consentire o bloccare le richieste in base al fatto che le richieste sembrano contenere codice SQL dannoso, crea condizioni di corrispondenza SQL injection. Per ulteriori informazioni, consulta Utilizzo di condizioni di corrispondenza SQL injection.
- Per consentire o bloccare le richieste in base alle stringhe visualizzate nelle richieste, crea condizioni di corrispondenza stringa. Per ulteriori informazioni, consulta Utilizzo di condizioni di corrispondenza per stringa.
- Per consentire o bloccare le richieste in base al modello regex visualizzato nelle richieste, crea condizioni di corrispondenza per regex. Per ulteriori informazioni, consulta Utilizzo di condizioni di corrispondenza per regex.

Argomenti

Utilizzo di condizioni di corrispondenza Cross-site scripting

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

A volte gli aggressori inseriscono script nelle richieste Web nel tentativo di sfruttare le vulnerabilità delle applicazioni Web. È possibile creare una o più condizioni di corrispondenza tra gli script tra siti per identificare le parti delle richieste Web, come l'URI o la stringa di query, che si desidera che AWS WAF Classic analizzi per individuare eventuali script dannosi. In un secondo momento, quando crei

un'ACL Web, specifichi se desideri consentire o bloccare le richieste che sembrano contenere script dannosi.

Argomenti

Creazione di condizioni di corrispondenza Cross-site scripting

Quando crei condizioni di corrispondenza Cross-site scripting, specifichi i filtri. I filtri indicano la parte di richieste Web che AWS WAF Classic deve ispezionare per rilevare la presenza di script dannosi, come l'URI o la stringa di query. È possibile aggiungere più di un filtro a una condizione di corrispondenza Cross-site scripting oppure è possibile creare una condizione separata per ogni filtro. Ecco come ogni configurazione influisce sul comportamento di AWS WAF Classic:

- Più di un filtro per condizione di corrispondenza tra siti di scripting (consigliato): quando aggiungi una condizione di corrispondenza tra siti scripting che contiene più filtri a una regola e aggiungi la regola a un ACL Web, una richiesta Web deve corrispondere solo a uno dei filtri nella condizione Cross-Scripting Match per AWS WAF Classic per consentire o bloccare la richiesta in base a tale condizione.

  Ad esempio, supponiamo di creare una condizione di corrispondenza Cross-site scripting e che la condizione contenga due filtri. Un filtro indica a AWS WAF Classic di ispezionare l'URI alla ricerca di script dannosi e l'altro indica a AWS WAF Classic di ispezionare la stringa di query. AWS WAF Classic consente o blocca le richieste se sembrano contenere script dannosi nell'URI o nella stringa di query.
- Un filtro per condizione di corrispondenza tra siti di scripting: quando si aggiungono condizioni di corrispondenza separate per lo scripting cross-site scripting a una regola e si aggiunge la regola a un ACL Web, le richieste Web devono soddisfare tutte le condizioni affinché AWS WAF Classic consenta o blocchi le richieste in base alle condizioni.

  Supponiamo di creare due condizione e ogni condizione contenga uno dei due filtri dell'esempio precedente. Quando aggiungi entrambe le condizioni alla stessa regola e aggiungi la regola a un

ACL Web, AWS WAF Classic consente o blocca le richieste solo quando sia l'URI che la stringa di query sembrano contenere script dannosi.

> **Note**
>
> Quando aggiungi una condizione di compatibilità tra siti di scripting a una regola, puoi anche configurare AWS WAF Classic per consentire o bloccare le richieste Web che non sembrano contenere script dannosi.

Per creare una condizione di corrispondenza Cross-site scripting

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere Cross-site scripting.
3. Scegliere Create condition (Crea condizione).
4. Specificare le impostazioni di filtro applicabili. Per ulteriori informazioni, consulta Valori da specificare durante la creazione o la modifica di condizioni di corrispondenza Cross-site scripting.
5. Scegliere Add another filter (Aggiungi un altro filtro).
6. Se si desidera aggiungere un altro filtro, ripetere le fasi 4 e 5.
7. Dopo aver aggiunto i filtri, selezionare Create (Crea).

Valori da specificare durante la creazione o la modifica di condizioni di corrispondenza Cross-site scripting

Quando crei o aggiorni una condizione di corrispondenza Cross-site scripting, specifichi i valori seguenti:

Nome

Il nome della condizione di corrispondenza Cross-site scripting.

Il nome può contenere solo caratteri A - Z, a - z, 0 - 9 e i caratteri speciali: _-!"#`+*},./ . Non è possibile modificare il nome di una condizione dopo averla creata.

Parte della richiesta su cui applicare un filtro

Scegli la parte di ogni richiesta web che vuoi che AWS WAF Classic esamini alla ricerca di script dannosi:

Header

Un'intestazione della richiesta specificata, ad esempio, l'intestazione `User-Agent` o `Referer`. Se scegli Header (Intestazione), specifica il nome dell'intestazione nel campo Header (Intestazione).

Metodo HTTP

Il metodo HTTP, che indica il tipo di operazione che la richiesta chiede all'origine di eseguire. CloudFront supporta i seguenti metodi: `DELETEGET`,`HEAD`, `OPTIONSPATCH`,`POST`, e`PUT`.

Stringa di query

La parte di un URL che viene visualizzata dopo un carattere `?`, se presente.

> **Note**
>
> Per le condizioni di corrispondenza Cross-site scripting, si consiglia di scegliere All query parameters (values only) (Tutti i parametri di query (solo valori)) invece di Query string (Stringa di query) per Part of the request to filter on (Parte della richiesta su cui filtrare).

URI

Il percorso URI della richiesta, che identifica la risorsa, `/images/daily-ad.jpg` ad esempio. Ciò non include la stringa di query o i componenti del frammento dell'URI. Per informazioni, vedete Uniform Resource Identifier (URI): sintassi generica.

A meno che non venga specificata una trasformazione, un URI non viene normalizzato e viene ispezionato non appena lo AWS riceve dal client come parte della richiesta. Un valore in Transformation (Trasformazione) riformatterà l'URI come specificato.

Body

La parte di una richiesta che contiene i dati aggiuntivi da inviare al server Web come corpo della richiesta HTTP, come i dati provenienti da un modulo.

> **Note**
>
> Se scegliete Body come valore di Parte della richiesta su cui filtrare, AWS WAF Classic ispeziona solo i primi 8192 byte (8 KB). Per consentire o bloccare le richieste il cui corpo è più lungo di 8192 byte, puoi creare una condizione di vincolo di dimensione. (AWS WAF Classic ottiene la lunghezza del corpo dalle intestazioni della richiesta.) Per ulteriori informazioni, consulta Utilizzo di condizioni per i vincoli di dimensioni.

Parametro di query singola (solo valore)

Qualsiasi parametro che hai definito come parte della stringa di query. Ad esempio, se l'URL è «www.xyz.com? UserName =abc& SalesRegion =seattle» puoi aggiungere un filtro al parametro or. UserNameSalesRegion

Se scegli Single query parameter (value only) (Parametro di query singola (solo valore)), sarà necessario anche specificare un valore in Query parameter name (Nome di parametro query). Questo è il parametro nella stringa di query che esaminerai, ad esempio o. UserNameSalesRegion La lunghezza massima per Query parameter name (Nome di parametro query) è 30 caratteri. Query parameter name (Nome di parametro query) non opera distinzione tra maiuscole e minuscole. Ad esempio, se si specifica UserNamecome nome del parametro Query, questo corrisponderà a tutte le varianti di UserName, come username e UserName.

Tutti i parametri di query (solo valori)

Analogamente al parametro Single query (solo valore), ma anziché esaminare i valori di un singolo parametro, AWS WAF Classic esamina tutti i valori dei parametri all'interno della stringa di query per individuare possibili script dannosi. Ad esempio, se l'URL è «www.xyz.com? UserName =abc& SalesRegion =seattle» e scegli Tutti i parametri di query (solo valori), AWS WAF Classic attiverà una corrispondenza se il valore di o contiene possibili script dannosi. UserNameSalesRegion

Header

Se hai scelto Intestazione per parte della richiesta su cui filtrare, scegli un'intestazione dall'elenco delle intestazioni comuni o inserisci il nome di un'intestazione che desideri che AWS WAF Classic controlli per individuare eventuali script dannosi.

Trasformazione

Una trasformazione riformatta una richiesta web prima che Classic la esamini. AWS WAF Ciò elimina parte della formattazione insolita utilizzata dagli aggressori nelle richieste Web nel tentativo di aggirare la versione classica. AWS WAF

È possibile specificare solo un unico tipo di trasformazione del testo.

Questo è in grado di eseguire le operazioni descritte di seguito:

Nessuno

AWS WAF Classic non esegue alcuna trasformazione di testo sulla richiesta Web prima di controllarla per verificare che la stringa in Value corrisponda.

Conversione in minuscolo

AWS WAF La versione classica converte le lettere maiuscole (A-Z) in minuscole (a-z).

Decodifica HTML

AWS WAF Classic sostituisce i caratteri con codifica HTML con caratteri non codificati:

- Sostituisce `&quot;` con &
- Sostituisce ` ` con uno spazio unificatore
- Sostituisce `<` con <
- Sostituisce `>` con >
- Sostituisce i caratteri rappresentati in formato esadecimale, `&#xhhhh;`, con i caratteri corrispondenti
- Sostituisce i caratteri rappresentati in formato decimale, `&#nnnn;`, con i caratteri corrispondenti

Normalizza lo spazio vuoto

AWS WAF Classic sostituisce i seguenti caratteri con uno spazio (decimale 32):

- \f, alimentazione modulo, decimale 12
- \t, tabulazione, decimale 9
- \n, nuova riga, decimale 10
- \r, ritorno a capo, decimale 13
- \v, tabulazione verticale, decimale 11
- spazio unificatore, decimale 160

Inoltre, questa opzione sostituisce più spazi con uno spazio.

Semplificazione della riga di comando

Per le richieste che contengono comandi della riga di comando del sistema operativo, utilizza questa opzione per eseguire le seguenti trasformazioni:

- Elimina i seguenti caratteri: \ " ' ^
- Eliminare gli spazi prima dei seguenti caratteri: / (
- Sostituire i seguenti caratteri con uno spazio: , ;
- Sostituire più spazi con uno spazio
- Convertire le lettere maiuscole (A-Z) in lettere minuscole (a-z)

Decodifica URL

Decodifica una richiesta con codifica URL.

Aggiunta ed eliminazione di filtri in una condizione di corrispondenza Cross-site scripting

È possibile aggiungere a una condizione di corrispondenza Cross-site scripting o eliminare filtri. Per modificare un filtro, aggiungine uno nuovo ed elimina il precedente.

Per aggiungere o eliminare filtri in una condizione di corrispondenza Cross-site scripting

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere Cross-site scripting.
3. Scegliere la condizione a aggiungere o da cui eliminare i filtri.
4. Per aggiungere filtri, procedere nel seguente modo:

   a. Scegliere Add filter (Aggiungi filtro).
   b. Specificare le impostazioni di filtro applicabili. Per ulteriori informazioni, consulta Valori da specificare durante la creazione o la modifica di condizioni di corrispondenza Cross-site scripting.
   c. Scegliere Aggiungi.
5. Per eliminare filtri, procedere nel seguente modo:

   a. Selezionare il filtro da eliminare.

b. Scegli Delete filter (Elimina filtro).

Eliminazione di condizioni di corrispondenza Cross-site scripting

Se desideri eliminare una condizione di corrispondenza Cross-site scripting, è necessario prima eliminare tutti i filtri nella condizione e rimuovere la condizione da tutte le regole che la utilizzano, come descritto nella seguente procedura.

Per eliminare una condizione di corrispondenza Cross-site scripting

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere Cross-site scripting.
3. Nel riquadro Cross-site scripting match conditions (Condizioni di corrispondenza Cross-site scripting), scegliere la condizione di corrispondenza Cross-site scripting da eliminare.
4. Nel riquadro a destra, scegliere la scheda Associated rules (Regole associate).

   Se l'elenco di regole che utilizza questa condizione di corrispondenza Cross-site scripting è vuoto, passare alla fase 6. Se l'elenco contiene regole, prendere nota delle regole e continuare con la fase 5.
5. Per rimuovere la condizione di corrispondenza Cross-site scripting dalle regole che la utilizzano, procedere nel seguente modo:

   a. Nel pannello di navigazione, scegli Regole.

   b. Scegliere il nome di una regola che utilizza la condizione di corrispondenza Cross-site scripting da eliminare.

   c. Nel riquadro a destra, selezionare la condizione di corrispondenza Cross-site scripting che si desidera rimuovere dalla regola e scegliere Remove selected condition (Rimuovi condizione selezionata).

   d. Ripetere le fasi b e c per tutte le regole rimanenti che utilizzano la condizione di corrispondenza Cross-site scripting da eliminare.

   e. Nel riquadro di navigazione, scegliere Cross-site scripting.

   f. Nel riquadro Cross-site scripting match conditions (Condizioni di corrispondenza Cross-site scripting), scegliere la condizione di corrispondenza Cross-site scripting da eliminare.

6. Scegliere Delete (Elimina) per eliminare la condizione selezionata.

Utilizzo di condizioni di corrispondenza IP

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Se desideri consentire o bloccare le richieste Web in base a gli indirizzi IP da cui hanno origine le richieste, crea condizioni di corrispondenza IP. Una condizione di corrispondenza IP elenca fino a 10.000 indirizzi IP o intervalli dell'indirizzo IP da cui hanno origine le richieste. In un secondo momento, quando crei un'ACL Web, specifichi se desideri consentire o bloccare le richieste da questi indirizzi IP.

Argomenti

- Creazione di una condizione di corrispondenza IP
- Modifica delle condizioni di corrispondenza IP
- Eliminazione delle condizioni di corrispondenza IP

Creazione di una condizione di corrispondenza IP

Se desideri consentire alcune richieste Web e bloccarne altre in base agli indirizzi IP da cui hanno origine le richieste, crea una condizione di corrispondenza IP per gli indirizzi IP da consentire e un'altra condizione di corrispondenza IP per gli indirizzi IP da bloccare.

> **Note**
>
> Quando aggiungi una condizione di corrispondenza IP a una regola, puoi anche configurare AWS WAF Classic per consentire o bloccare le richieste Web che non provengono dagli indirizzi IP specificati nella condizione.

Per creare una condizione di corrispondenza IP

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere IP addresses (Indirizzi IP).
3. Scegliere Create condition (Crea condizione).
4. Immettere un nome nel campo Name (Nome) .

   Il nome può contenere solo caratteri alfanumerici (A - Z, a - z, 0 - 9) o i seguenti caratteri speciali: _-!"#`+*},./ . Non è possibile modificare il nome di una condizione dopo averla creata.
5. Selezionare la versione IP corretta e specificare un indirizzo IP o un intervallo di indirizzi IP usando la notazione CIDR. Ecco alcuni esempi:

   - Per specificare l'indirizzo IPv4 192.0.2.44, digitare 192.0.2.44/32.
   - Per specificare l'indirizzo IPv6 0:0:0:0:0:ffff:c000:22c, digitare 0:0:0:0:0:ffff:c000:22c/128.
   - Per specificare l'intervallo di indirizzi IPv4 da 192.0.2.0 a 192.0.2.255, digitare 192.0.2.0/24.
   - Per specificare l'intervallo di indirizzi IPv6 da 2620:0:2d0:200:0:0:0:0 a 2620:0:2d0:200:ffff:ffff:ffff:ffff, immettere 2620:0:2d0:200::/64.

   AWS WAF Classic supporta gli intervalli di indirizzi IPv4: /8 e qualsiasi intervallo compreso tra /16 e /32. AWS WAF Classic supporta gli intervalli di indirizzi IPv6: /24, /32, /48, /56, /64 e /128. Per ulteriori informazioni sulla notazione CIDR, consulta la voce Classless Inter-Domain Routing su Wikipedia.
6. Scegliere Add another IP address or range (Aggiungi un altro intervallo o indirizzo IP).
7. Se si desidera aggiungere un altro intervallo o un altro indirizzo IP, ripetere le fasi 5 e 6.
8. Dopo aver aggiunto i valori, scegliere Create IP match condition (Crea condizione di corrispondenza IP).

Modifica delle condizioni di corrispondenza IP

È possibile aggiungere un intervallo di indirizzi IP a una condizione di corrispondenza IP o eliminare un intervallo. Per modificare un intervallo, aggiungine uno nuovo ed elimina il precedente.

Per modificare una condizione di corrispondenza IP

1. Accedi e apri la console all'indirizzo https://console.aws.amazon.com/wafv2/. AWS Management ConsoleAWS WAF

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere IP addresses (Indirizzi IP).
3. Nel riquadro IP match conditions (condizioni di corrispondenza IP) scegliere la condizione di corrispondenza IP che si desidera modificare.
4. Per aggiungere un intervallo di indirizzi IP:

   a. Nel riquadro di destra, scegliere Add IP address or range (Aggiungi intervallo o indirizzo IP).

   b. Selezionare la versione IP corretta e immettere un intervallo di indirizzi IP usando la notazione CIDR. Ecco alcuni esempi:

      - Per specificare l'indirizzo IPv4 192.0.2.44, immettere 192.0.2.44/32.
      - Per specificare l'indirizzo IPv6 0:0:0:0:0:ffff:c000:22c, immettere 0:0:0:0:0:ffff:c000:22c/128.
      - Per specificare l'intervallo di indirizzi IPv4 da 192.0.2.0 a 192.0.2.255, immettere 192.0.2.0/24.
      - Per specificare l'intervallo di indirizzi IPv6 da 2620:0:2d0:200:0:0:0:0 a 2620:0:2d0:200:ffff:ffff:ffff:ffff, immettere 2620:0:2d0:200::/64.

      AWS WAF Classic supporta gli intervalli di indirizzi IPv4: /8 e qualsiasi intervallo compreso tra /16 e /32. AWS WAF Classic supporta gli intervalli di indirizzi IPv6: /24, /32, /48, /56, /64 e /128. Per ulteriori informazioni sulla notazione CIDR, consulta la voce Classless Inter-Domain Routing su Wikipedia.

   c. Per aggiungere ulteriori indirizzi IP, scegliere Add another IP address (Aggiungi un altro indirizzo IP) e immettere il valore.

   d. Scegli Aggiungi.
5. Per eliminare un intervallo o un indirizzo IP:

   a. Nel riquadro a destra, selezionare i valori da eliminare.

   b. Scegliere Delete IP address or range (Elimina indirizzo IP o intervallo).

Eliminazione delle condizioni di corrispondenza IP

Se desideri eliminare una condizione di corrispondenza IP, è necessario prima eliminare tutti gli intervalli e gli indirizzi IP nella condizione e rimuovere la condizione da tutte le regole che la utilizzano, come descritto nella seguente procedura.

Per eliminare una condizione di corrispondenza IP

1. Accedi e apri la console all'indirizzo https://console.aws.amazon.com/wafv2/. AWS Management ConsoleAWS WAF

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere IP addresses (Indirizzi IP).
3. Nel riquadro IP match conditions (Condizioni di corrispondenza IP), scegliere la condizione di corrispondenza IP da eliminare.
4. Nel riquadro a destra, scegliere la scheda Rules (Regolamento).

   Se l'elenco di regole che utilizza questa condizione di corrispondenza IP è vuoto, passare alla fase 6. Se l'elenco contiene regole, prendere nota delle regole e continuare con la fase 5.
5. Per rimuovere la condizione di corrispondenza IP dalle regole che la utilizzano, procedere nel seguente modo:

   a. Nel pannello di navigazione, scegli Regole.

   b. Scegliere il nome di una regola che utilizza la condizione di corrispondenza IP da eliminare.

   c. Nel riquadro a destra, selezionare la condizione di corrispondenza IP che si desidera rimuovere dalla regola e scegliere Remove selected condition (Rimuovi condizione selezionata).

   d. Ripetere le fasi b e c per tutte le regole rimanenti che utilizzano la condizione di corrispondenza IP da eliminare.

   e. Nel riquadro di navigazione, scegliere IP match conditions (Condizioni di corrispondenza IP).

   f. Nel riquadro IP match conditions (Condizioni di corrispondenza IP), scegliere la condizione di corrispondenza IP da eliminare.
6. Scegliere Delete (Elimina) per eliminare la condizione selezionata.

Utilizzo di condizioni di corrispondenza geografica

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Se desideri consentire o bloccare le richieste Web in base al paese da cui hanno origine le richieste, crea condizioni di corrispondenza geografica. Una condizione di corrispondenza geografica elenca i paesi da cui hanno origine le richieste. In un secondo momento, quando crei un'ACL Web, specifichi se desideri consentire o bloccare le richieste da questi paesi.

Puoi utilizzare le condizioni di geo match con altre condizioni o regole AWS WAF classiche per creare filtri sofisticati. Ad esempio, se desideri bloccare determinati paesi, ma consentire comunque indirizzi IP specifici da quel paese, è possibile creare una regola contenente una condizione di corrispondenza geografica e una condizione di corrispondenza IP. Configura la regola per bloccare le richieste che hanno origine da quel paese e non corrispondono agli indirizzi IP approvati. Un altro esempio, se desideri assegnare la priorità alle risorse per gli utenti in un determinato paese, è possibile includere una condizione di corrispondenza geografica in due diverse regole basate sulla frequenza. Imposta un limite di frequenza più elevato per gli utenti nel paese preferito e imposta un limite di frequenza inferiore per tutti gli altri utenti.

> **Note**
>
> Se utilizzi la funzione di restrizione CloudFront geografica per impedire a un paese di accedere ai tuoi contenuti, qualsiasi richiesta proveniente da quel paese viene bloccata e non viene inoltrata a Classic. AWS WAF Pertanto, se desideri consentire o bloccare le richieste in base alla geografia e ad altre condizioni della AWS WAF versione classica, non dovresti utilizzare la funzione di restrizione geografica. CloudFront Invece, dovresti usare una condizione di geo AWS WAF match classica.

Argomenti

- Creazione di una condizione di corrispondenza geografica

- Modifica delle condizioni di corrispondenza geografica
- Eliminazione delle condizioni di corrispondenza geografica

Creazione di una condizione di corrispondenza geografica

Se desideri consentire alcune richieste Web e bloccarne altre in base ai paesi da cui hanno origine le richieste, crea una condizione di corrispondenza geografica per i paesi da consentire e un'altra condizione di corrispondenza geografica per i paesi da bloccare.

> **Note**
>
> Quando aggiungi una condizione di corrispondenza geografica a una regola, puoi anche configurare AWS WAF Classic per consentire o bloccare le richieste Web che non provengono dal paese specificato nella condizione.

Per creare una condizione di corrispondenza geografica

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere Geo match (Corrispondenza geografica).
3. Scegliere Create condition (Crea condizione).
4. Immettere un nome nel campo Name (Nome) .

   Il nome può contenere solo caratteri alfanumerici (A - Z, a - z, 0 - 9) o i seguenti caratteri speciali: _-!"#`+*},./ . Non è possibile modificare il nome di una condizione dopo averla creata.
5. Scegliere una Region (Regione).
6. Scegliere un Location type (Tipo di luogo) e un paese. Location type (Tipo di posizione) può essere attualmente solo Country (Paese).
7. Scegliere Add location (Aggiungi luogo).
8. Scegli Crea.

Modifica delle condizioni di corrispondenza geografica

È possibile aggiungere paesi o eliminare paesi dalla condizione di corrispondenza geografica.

Per modificare una condizione di corrispondenza geografica

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere Geo match (Corrispondenza geografica).
3. Nel riquadro Geo match conditions (Condizioni di corrispondenza geografica), scegliere la condizione di corrispondenza geografica da modificare.
4. Per aggiungere un paese:
   a. Nel riquadro a destra, scegliere Add filter (Aggiungi filtro).
   b. Scegliere un Location type (Tipo di luogo) e un paese. Location type (Tipo di posizione) può essere attualmente solo Country (Paese).
   c. Scegli Aggiungi.
5. Per eliminare un paese:
   a. Nel riquadro a destra, selezionare i valori da eliminare.
   b. Scegli Delete filter (Elimina filtro).

Eliminazione delle condizioni di corrispondenza geografica

Se desideri eliminare una condizione di corrispondenza geografica, è necessario prima rimuovere tutti i paesi nella condizione e rimuovere la condizione da tutte le regole che la utilizzano, come descritto nella seguente procedura.

Per eliminare una condizione di corrispondenza geografica

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Rimuovere la condizione di corrispondenza geografica dalle regole che la utilizzano:
   a. Nel pannello di navigazione, scegli Regole.
   b. Scegliere il nome di una regola che utilizza la condizione di corrispondenza geografica da eliminare.

c. Nel riquadro a destra, selezionare Edit rule (Modifica regola).
d. Scegliere la X accanto alla condizione da eliminare.
e. Scegli Aggiorna.
f. Ripetere per tutte le regole rimanenti che utilizzano la condizione di corrispondenza geografica da eliminare.

3. Rimuovere i filtri dalla condizione da eliminare:

a. Nel riquadro di navigazione, scegliere Geo match (Corrispondenza geografica).
b. Scegli il nome della condizione di corrispondenza geografica da eliminare.
c. Nel riquadro a destra, scegliere la casella di controllo accanto a Filter (Filtro) per selezionare tutti i filtri.
d. Scegliere Delete filter (Elimina filtro).

4. Nel riquadro di navigazione, scegliere Geo match (Corrispondenza geografica).
5. Nel riquadro Geo match conditions (Condizioni di corrispondenza geografica), scegliere la condizione di corrispondenza geografica da eliminare.
6. Scegliere Delete (Elimina) per eliminare la condizione selezionata.

Utilizzo di condizioni per i vincoli di dimensioni

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Se desideri consentire o bloccare le richieste Web in base alla lunghezza delle parti specificate della richiesta, crea una o più condizioni per i vincoli di dimensioni. Una condizione di vincolo di dimensione identifica la parte di richieste Web che si desidera che AWS WAF Classic esamini, il numero di byte che deve cercare AWS WAF Classic e un operatore, ad esempio maggiore di (>) o minore di (<). Ad esempio, è possibile utilizzare una condizione per i vincoli di dimensioni per cercare stringhe di query con più di 100 byte. In un secondo momento, quando crei un'ACL Web, specifichi se desideri consentire o bloccare le richieste in base a quelle impostazioni.

Tieni presente che se configuri AWS WAF Classic per ispezionare il corpo della richiesta, ad esempio cercando nel corpo una stringa specificata, AWS WAF Classic ispeziona solo i primi 8192 byte (8 KB). Se il corpo della richiesta per le richieste Web non supera mai 8.192 byte, è possibile creare una condizione per i vincoli di dimensioni e bloccare le richieste con un corpo di richiesta maggiore di 8.192 byte.

Argomenti

Creazione di condizioni per i vincoli di dimensioni

Quando si creano condizioni di vincolo di dimensione, si specificano filtri che identificano la parte delle richieste Web di cui si desidera AWS WAF che Classic valuti la lunghezza. È possibile aggiungere più di un filtro a una condizione per i vincoli di dimensioni oppure è possibile creare una condizione separata per ogni filtro. Ecco come ogni configurazione influisce sul comportamento di AWS WAF Classic:

- Un filtro per condizione di vincolo di dimensione: quando aggiungi condizioni di vincolo di dimensione separate a una regola e aggiungi la regola a un ACL Web, le richieste Web devono soddisfare tutte le condizioni affinché AWS WAF Classic consenta o blocchi le richieste in base alle condizioni.

  Ad esempio, supponiamo che crei due condizioni. Una corrisponde alle richieste Web per le quali le stringhe di query sono maggiori di 100 byte. L'altra corrisponde alle richieste Web per le quali il corpo della richiesta è maggiore di 1.024 byte. Quando aggiungi entrambe le condizioni alla stessa regola e aggiungi la regola a un ACL web, AWS WAF Classic consente o blocca le richieste solo quando entrambe le condizioni sono vere.
- Più di un filtro per condizione di vincolo di dimensione: quando aggiungi una condizione di vincolo di dimensione che contiene più filtri a una regola e aggiungi la regola a un ACL Web, una richiesta Web deve corrispondere solo a uno dei filtri nella condizione di vincolo di dimensione per AWS WAF Classic per consentire o bloccare la richiesta in base a tale condizione.

Supponiamo di creare una condizione anziché due e che l'unica condizione contenga gli stessi due filtri dell'esempio precedente. AWS WAF La versione classica consente o blocca le richieste se la stringa di query è superiore a 100 byte o il corpo della richiesta è maggiore di 1024 byte.

> **Note**
>
> Quando aggiungi una condizione di vincolo di dimensione a una regola, puoi anche configurare AWS WAF Classic per consentire o bloccare le richieste Web che non corrispondono ai valori della condizione.

Per creare una condizione per i vincoli di dimensioni

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere Size constraints (Vincoli di dimensione).
3. Scegliere Create condition (Crea condizione).
4. Specificare le impostazioni di filtro applicabili. Per ulteriori informazioni, consulta Valori da specificare durante la creazione o la modifica di condizioni per i vincoli di dimensioni.
5. Scegliere Add another filter (Aggiungi un altro filtro).
6. Se si desidera aggiungere un altro filtro, ripetere le fasi 4 e 5.
7. Dopo aver aggiunto i filtri, scegliere Create size constraint condition (Crea condizione per i vincoli di dimensioni).

Valori da specificare durante la creazione o la modifica di condizioni per i vincoli di dimensioni

Quando crei o aggiorni una condizione per i vincoli di dimensioni, specifichi i valori seguenti:

Nome

Immetti un nome per la condizione per i vincoli di dimensioni.

Il nome può contenere solo caratteri alfanumerici (A - Z, a - z, 0 - 9) o i seguenti caratteri speciali: _-!"#`+*},./. Non è possibile modificare il nome di una condizione dopo averla creata.

Parte della richiesta su cui applicare un filtro

Scegli la parte di ogni richiesta web per la quale desideri che AWS WAF Classic valuti la lunghezza:

Header

Un'intestazione della richiesta specificata, ad esempio, l'intestazione `User-Agent` o `Referer`. Se scegli Header (Intestazione), specifica il nome dell'intestazione nel campo Header (Intestazione).

Metodo HTTP

Il metodo HTTP, che indica il tipo di operazione che la richiesta chiede all'origine di eseguire. CloudFront supporta i seguenti metodi: `DELETEGET`,`HEAD`, `OPTIONSPATCH`,`POST`, e`PUT`.

Stringa di query

La parte di un URL che viene visualizzata dopo un carattere `?`, se presente.

URI

Il percorso URI della richiesta, che identifica la risorsa, `/images/daily-ad.jpg` ad esempio. Ciò non include la stringa di query o i componenti del frammento dell'URI. Per informazioni, vedete Uniform Resource Identifier (URI): sintassi generica.

A meno che non venga specificata una trasformazione, un URI non viene normalizzato e viene ispezionato non appena lo AWS riceve dal client come parte della richiesta. Un valore in Transformation (Trasformazione) riformatterà l'URI come specificato.

Body

La parte di una richiesta che contiene i dati aggiuntivi da inviare al server Web come corpo della richiesta HTTP, come i dati provenienti da un modulo.

Parametro di query singola (solo valore)

Qualsiasi parametro che hai definito come parte della stringa di query. Ad esempio, se l'URL è «www.xyz.com? UserName =abc& SalesRegion =seattle» puoi aggiungere un filtro al parametro or. UserNameSalesRegion

Se scegli Single query parameter (value only) (Parametro di query singola (solo valore)), sarà necessario anche specificare un valore in Query parameter name (Nome di parametro

query). Questo è il parametro nella stringa di query che esaminerai, ad esempio. UserName La lunghezza massima per Query parameter name (Nome di parametro query) è 30 caratteri. Query parameter name (Nome di parametro query) non opera distinzione tra maiuscole e minuscole. Ad esempio, se si specifica UserNamecome nome del parametro Query, questo corrisponderà a tutte le varianti di UserName, come username e UserName.

Tutti i parametri di query (solo valori)

Analogamente al parametro Single query (solo valore), ma anziché controllare il valore di un singolo parametro, AWS WAF Classic esamina i valori di tutti i parametri all'interno della stringa di query per verificare il vincolo di dimensione. Ad esempio, se l'URL è «www.xyz.com? UserName =abc& SalesRegion =seattle» e scegli Tutti i parametri di query (solo valori), AWS WAF Classic attiverà una corrispondenza con il valore se uno dei due o supera la dimensione specificata. UserNameSalesRegion

Intestazione (solo quando la "Part of the request to filter on (Parte della richiesta sulla quale filtrare)" è "Header (Intestazione)")

Se hai scelto Intestazione per parte della richiesta su cui filtrare, scegli un'intestazione dall'elenco delle intestazioni comuni o digita il nome di un'intestazione di cui desideri che Classic valuti la lunghezza. AWS WAF

Operatore di confronto

Scegliete come desiderate che AWS WAF Classic valuti la lunghezza della stringa di query nelle richieste Web rispetto al valore specificato per Size.

Ad esempio, se scegliete È maggiore di per l'operatore di confronto e digitate 100 per Dimensione, AWS WAF Classic valuta le richieste Web per una stringa di query più lunga di 100 byte.

Size

Immettete la lunghezza, in byte, che AWS WAF Classic deve controllare nelle stringhe di query.

> **Note**
>
> Se scegli URI per il valore di Part of the request to filter on (Parte della richiesta sulla quale filtrare), / nell'URI conta come un carattere. Ad esempio, il percorso URI `/logo.jpg` è lungo nove caratteri.

Trasformazione

Una trasformazione riformatta una richiesta Web prima che AWS WAF Classic valuti la lunghezza della parte specificata della richiesta. Ciò elimina parte della formattazione insolita utilizzata dagli aggressori nelle richieste Web nel tentativo di aggirare la versione classica. AWS WAF

> **Note**
>
> Se scegli Body for Part della richiesta su cui filtrare, non puoi configurare AWS WAF Classic per eseguire una trasformazione perché solo i primi 8192 byte vengono inoltrati per l'ispezione. Tuttavia, puoi comunque filtrare il traffico in base alla dimensione del corpo della richiesta HTTP e specificare una trasformazione di Nessuno. (AWS WAF Classic ottiene la lunghezza del corpo dalle intestazioni della richiesta.)

È possibile specificare solo un unico tipo di trasformazione del testo.

Questo è in grado di eseguire le operazioni descritte di seguito:

Nessuno

AWS WAF Classic non esegue alcuna trasformazione di testo sulla richiesta Web prima di verificarne la lunghezza.

Conversione in minuscolo

AWS WAF La versione classica converte le lettere maiuscole (A-Z) in minuscole (a-z).

Decodifica HTML

AWS WAF Classic sostituisce i caratteri con codifica HTML con caratteri non codificati:

- Sostituisce `&quot;` con `&`
- Sostituisce ` ` con uno spazio unificatore
- Sostituisce `<` con `<`
- Sostituisce `>` con `>`
- Sostituisce i caratteri rappresentati in formato esadecimale, `&#xhhhh;`, con i caratteri corrispondenti
- Sostituisce i caratteri rappresentati in formato decimale, `&#nnnn;`, con i caratteri corrispondenti

Normalizza lo spazio vuoto

AWS WAF Classic sostituisce i seguenti caratteri con uno spazio (decimale 32):

- \f, alimentazione modulo, decimale 12
- \t, tabulazione, decimale 9
- \n, nuova riga, decimale 10
- \r, ritorno a capo, decimale 13
- \v, tabulazione verticale, decimale 11
- spazio unificatore, decimale 160

Inoltre, questa opzione sostituisce più spazi con uno spazio.

Semplificazione della riga di comando

Per le richieste che contengono comandi della riga di comando del sistema operativo, utilizza questa opzione per eseguire le seguenti trasformazioni:

- Elimina i seguenti caratteri: \ " ' ^
- Eliminare gli spazi prima dei seguenti caratteri: / (
- Sostituire i seguenti caratteri con uno spazio: , ;
- Sostituire più spazi con uno spazio
- Convertire le lettere maiuscole (A-Z) in lettere minuscole (a-z)

Decodifica URL

Decodifica una richiesta con codifica URL.

Aggiunta ed eliminazione di filtri in una condizione per i vincoli di dimensioni

È possibile aggiungere a una condizione per i vincoli di dimensioni o eliminare filtri. Per modificare un filtro, aggiungine uno nuovo ed elimina il precedente.

Per aggiungere o eliminare filtri in una condizione per i vincoli di dimensioni

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere Size constraints (Vincoli di dimensione).

3. Scegliere la condizione a aggiungere o da cui eliminare i filtri.
4. Per aggiungere filtri, procedere nel seguente modo:
   a. Scegliere Add filter (Aggiungi filtro).
   b. Specificare le impostazioni di filtro applicabili. Per ulteriori informazioni, consulta Valori da specificare durante la creazione o la modifica di condizioni per i vincoli di dimensioni.
   c. Scegliere Aggiungi.
5. Per eliminare filtri, procedere nel seguente modo:
   a. Selezionare il filtro da eliminare.
   b. Scegli Delete filter (Elimina filtro).

Eliminazione di condizioni per i vincoli di dimensioni

Se desideri eliminare una condizione per i vincoli di dimensioni, è necessario prima eliminare tutti i filtri nella condizione e rimuovere la condizione da tutte le regole che la utilizzano, come descritto nella seguente procedura.

Per eliminare una condizione per i vincoli di dimensioni

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere Size constraints (Vincoli di dimensione).
3. Nel riquadro Size constraint conditions (Condizioni per i vincoli di dimensioni), scegliere la condizione per i vincoli di dimensioni da eliminare.
4. Nel riquadro a destra, scegliere la scheda Associated rules (Regole associate).

   Se l'elenco di regole che utilizza questa condizione per i vincoli di dimensioni è vuoto, passare alla fase 6. Se l'elenco contiene regole, prendere nota delle regole e continuare con la fase 5.
5. Per rimuovere la condizione per i vincoli di dimensioni dalle regole che la utilizzano, procedere nel seguente modo:
   a. Nel pannello di navigazione, scegli Regole.
   b. Scegliere il nome di una regola che utilizza la condizione per i vincoli di dimensioni da eliminare.

c. Nel riquadro a destra, selezionare la condizione per i vincoli di dimensioni che si desidera rimuovere dalla regola e scegliere Remove selected condition (Rimuovi condizione selezionata).

d. Ripetere le fasi b e c per tutte le regole rimanenti che utilizzano la condizione per i vincoli di dimensioni da eliminare.

e. Nel riquadro di navigazione, scegliere Size constraints (Vincoli di dimensione).

f. Nel riquadro Size constraint conditions (Condizioni per i vincoli di dimensioni), scegliere la condizione per i vincoli di dimensioni da eliminare.

6. Scegliere Delete (Elimina) per eliminare la condizione selezionata.

Utilizzo di condizioni di corrispondenza SQL injection

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

A volte gli aggressori inseriscono codice SQL dannoso nelle richieste Web nel tentativo di estrarre dati dal database. Per consentire o bloccare le richieste Web che sembrano contenere codice SQL dannoso, crea una o più condizioni di corrispondenza SQL injection. Una condizione di SQL injection match identifica la parte delle richieste Web, ad esempio il percorso URI o la stringa di query, che AWS WAF Classic deve esaminare. In un secondo momento, quando crei un'ACL Web, specifichi se desideri consentire o bloccare le richieste che sembrano contenere codice SQL dannoso.

Argomenti

- Creazione di condizioni di corrispondenza SQL injection
- Valori da specificare durante la creazione o la modifica di condizioni di corrispondenza SQL injection
- Aggiunta ed eliminazione di filtri in una condizione di corrispondenza SQL injection
- Eliminazione di condizioni di corrispondenza SQL injection

Creazione di condizioni di corrispondenza SQL injection

Quando si creano condizioni di corrispondenza di SQL injection, si specificano i filtri, che indicano la parte di richieste Web che AWS WAF Classic deve ispezionare per rilevare la presenza di codice SQL dannoso, ad esempio l'URI o la stringa di query. È possibile aggiungere più di un filtro a una condizione di corrispondenza SQL injection oppure è possibile creare una condizione separata per ogni filtro. Ecco come ogni configurazione influisce sul comportamento di AWS WAF Classic:

- Più di un filtro per condizione di corrispondenza SQL Injection (consigliato): quando si aggiunge una condizione di SQL injection match contenente più filtri a una regola e si aggiunge la regola a un ACL Web, è sufficiente che una richiesta Web corrisponda a uno dei filtri nella condizione di SQL injection match per AWS WAF Classic per consentire o bloccare la richiesta in base a tale condizione.

  Ad esempio, supponiamo di creare una condizione di corrispondenza SQL injection e che la condizione contenga due filtri. Un filtro indica a AWS WAF Classic di ispezionare l'URI alla ricerca di codice SQL dannoso e l'altro indica a AWS WAF Classic di ispezionare la stringa di query. AWS WAF Classic consente o blocca le richieste se sembrano contenere codice SQL dannoso nell'URI o nella stringa di query.
- Un filtro per condizione di corrispondenza SQL Injection: quando si aggiungono condizioni di SQL injection match separate a una regola e si aggiunge la regola a un ACL Web, le richieste Web devono soddisfare tutte le condizioni affinché AWS WAF Classic consenta o blocchi le richieste in base alle condizioni.

  Supponiamo di creare due condizione e ogni condizione contenga uno dei due filtri dell'esempio precedente. Quando si aggiungono entrambe le condizioni alla stessa regola e si aggiunge la regola a un ACL Web, AWS WAF Classic consente o blocca le richieste solo quando sia l'URI che la stringa di query sembrano contenere codice SQL dannoso.

> **Note**
>
> Quando aggiungi una condizione di SQL injection match a una regola, puoi anche configurare AWS WAF Classic per consentire o bloccare le richieste Web che non sembrano contenere codice SQL dannoso.

Per creare condizione di corrispondenza SQL injection

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione scegliere SQL injection.
3. Scegliere Create condition (Crea condizione).
4. Specificare le impostazioni di filtro applicabili. Per ulteriori informazioni, consulta Valori da specificare durante la creazione o la modifica di condizioni di corrispondenza SQL injection.
5. Scegliere Add another filter (Aggiungi un altro filtro).
6. Se si desidera aggiungere un altro filtro, ripetere le fasi 4 e 5.
7. Dopo aver aggiunto i filtri, selezionare Create (Crea).

Valori da specificare durante la creazione o la modifica di condizioni di corrispondenza SQL injection

Quando crei o aggiorni una condizione di corrispondenza SQL injection specifichi i valori seguenti:

Nome

Il nome della condizione di corrispondenza SQL injection.

Il nome può contenere solo caratteri alfanumerici (A - Z, a - z, 0 - 9) o i seguenti caratteri speciali: _-!"#`+*},./. Non è possibile modificare il nome di una condizione dopo averla creata.

Parte della richiesta su cui applicare un filtro

Scegli la parte di ogni richiesta web che vuoi che AWS WAF Classic esamini alla ricerca di codice SQL dannoso:

Header

Un'intestazione della richiesta specificata, ad esempio, l'intestazione `User-Agent` o `Referer`. Se scegli Header (Intestazione), specifica il nome dell'intestazione nel campo Header (Intestazione).

Metodo HTTP

Il metodo HTTP, che indica il tipo di operazione che la richiesta chiede all'origine di eseguire. CloudFront supporta i seguenti metodi: `DELETEGET`,`HEAD`, `OPTIONSPATCH`,`POST`, e`PUT`.

Stringa di query

La parte di un URL che viene visualizzata dopo un carattere ?, se presente.

> **Note**
>
> Per le condizioni di corrispondenza SQL injection, si consiglia di scegliere All query parameters (values only) (Tutti i parametri di query (solo valori)) anziché Query string (Stringa di query) per Part of the request to filter on (Parte della richiesta su cui filtrare).

URI

Il percorso URI della richiesta, che identifica la risorsa, `/images/daily-ad.jpg` ad esempio. Ciò non include la stringa di query o i componenti del frammento dell'URI. Per informazioni, vedete Uniform Resource Identifier (URI): sintassi generica.

A meno che non venga specificata una trasformazione, un URI non viene normalizzato e viene ispezionato non appena lo AWS riceve dal client come parte della richiesta. Un valore in Transformation (Trasformazione) riformatterà l'URI come specificato.

Body

La parte di una richiesta che contiene i dati aggiuntivi da inviare al server Web come corpo della richiesta HTTP, come i dati provenienti da un modulo.

> **Note**
>
> Se scegliete Body come valore di Parte della richiesta su cui filtrare, AWS WAF Classic ispeziona solo i primi 8192 byte (8 KB). Per consentire o bloccare le richieste il cui corpo è più lungo di 8192 byte, puoi creare una condizione di vincolo di dimensione. (AWS WAF Classic ottiene la lunghezza del corpo dalle intestazioni della richiesta.) Per ulteriori informazioni, consulta Utilizzo di condizioni per i vincoli di dimensioni.

Parametro di query singola (solo valore)

Qualsiasi parametro che hai definito come parte della stringa di query. Ad esempio, se l'URL è «www.xyz.com? UserName =abc& SalesRegion =seattle» puoi aggiungere un filtro al parametro or. UserNameSalesRegion

Se scegli Single query parameter (value only) (Parametro di query singola (solo valore)), sarà necessario anche specificare un valore in Query parameter name (Nome di parametro query). Questo è il parametro nella stringa di query che esaminerai, ad esempio o. UserNameSalesRegion La lunghezza massima per Query parameter name (Nome di parametro query) è 30 caratteri. Query parameter name (Nome di parametro query) non opera distinzione tra maiuscole e minuscole. Ad esempio, se si specifica UserNamecome nome del parametro Query, questo corrisponderà a tutte le varianti di UserName, come username e UserName.

Tutti i parametri di query (solo valori)

Analogamente al parametro Single query (solo valore), ma anziché esaminare il valore di un singolo parametro, AWS WAF Classic esamina il valore di tutti i parametri all'interno della stringa di query per individuare eventuali codici SQL dannosi. Ad esempio, se l'URL è «www.xyz.com? UserName =abc& SalesRegion =seattle» e scegli Tutti i parametri di query (solo valori), AWS WAF Classic attiverà una corrispondenza se il valore di uno dei due o contiene un possibile codice SQL dannoso. UserNameSalesRegion

Header

Se hai scelto Intestazione per parte della richiesta su cui filtrare, scegli un'intestazione dall'elenco delle intestazioni comuni o inserisci il nome di un'intestazione che desideri che AWS WAF Classic controlli per rilevare la presenza di codice SQL dannoso.

Trasformazione

Una trasformazione riformatta una richiesta Web prima che Classic esamini la richiesta. AWS WAF Ciò elimina parte della formattazione insolita utilizzata dagli aggressori nelle richieste Web nel tentativo di aggirare la versione classica. AWS WAF

È possibile specificare solo un unico tipo di trasformazione del testo.

Questo è in grado di eseguire le operazioni descritte di seguito:

Nessuno

AWS WAF Classic non esegue alcuna trasformazione di testo sulla richiesta Web prima di controllarla per verificare che la stringa in Value corrisponda.

Conversione in minuscolo

AWS WAF La versione classica converte le lettere maiuscole (A-Z) in minuscole (a-z).

Decodifica HTML

AWS WAF Classic sostituisce i caratteri con codifica HTML con caratteri non codificati:

- Sostituisce `&quot;` con &
- Sostituisce ` ` con uno spazio unificatore
- Sostituisce `<` con <
- Sostituisce `>` con >
- Sostituisce i caratteri rappresentati in formato esadecimale, `&#xhhhh;`, con i caratteri corrispondenti
- Sostituisce i caratteri rappresentati in formato decimale, `&#nnnn;`, con i caratteri corrispondenti

Normalizza lo spazio vuoto

AWS WAF Classic sostituisce i seguenti caratteri con uno spazio (decimale 32):

- \f, alimentazione modulo, decimale 12
- \t, tabulazione, decimale 9
- \n, nuova riga, decimale 10
- \r, ritorno a capo, decimale 13
- \v, tabulazione verticale, decimale 11
- spazio unificatore, decimale 160

Inoltre, questa opzione sostituisce più spazi con uno spazio.

Semplificazione della riga di comando

Per le richieste che contengono comandi della riga di comando del sistema operativo, utilizza questa opzione per eseguire le seguenti trasformazioni:

- Elimina i seguenti caratteri: \ " ' ^
- Eliminare gli spazi prima dei seguenti caratteri: / (
- Sostituire i seguenti caratteri con uno spazio: , ;
- Sostituire più spazi con uno spazio
- Convertire le lettere maiuscole (A-Z) in lettere minuscole (a-z)

Decodifica URL

Decodifica una richiesta con codifica URL.

Aggiunta ed eliminazione di filtri in una condizione di corrispondenza SQL injection

È possibile aggiungere una condizione di corrispondenza SQL injection o eliminare filtri. Per modificare un filtro, aggiungine uno nuovo ed elimina il precedente.

Per aggiungere o eliminare filtri in una condizione di corrispondenza SQL injection

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione scegliere SQL injection.
3. Scegliere la condizione a aggiungere o da cui eliminare i filtri.
4. Per aggiungere filtri, procedere nel seguente modo:
   a. Scegliere Add filter (Aggiungi filtro).
   b. Specificare le impostazioni di filtro applicabili. Per ulteriori informazioni, consulta Valori da specificare durante la creazione o la modifica di condizioni di corrispondenza SQL injection.
   c. Scegliere Aggiungi.
5. Per eliminare filtri, procedere nel seguente modo:
   a. Selezionare il filtro da eliminare.
   b. Scegli Delete filter (Elimina filtro).

Eliminazione di condizioni di corrispondenza SQL injection

Se desideri eliminare una condizione di corrispondenza SQL injection, è necessario prima eliminare tutti i filtri nella condizione e rimuovere la condizione da tutte le regole che la utilizzano, come descritto nella seguente procedura.

Per eliminare una condizione di corrispondenza SQL injection

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione scegliere SQL injection.

3. Nel riquadro SQL injection match conditions (Condizioni di corrispondenza SQL injection), scegliere la condizione di corrispondenza SQL injection da eliminare.
4. Nel riquadro a destra, scegliere la scheda Associated rules (Regole associate).

   Se l'elenco di regole che utilizza questa condizione di corrispondenza SQL injection è vuoto, passare alla fase 6. Se l'elenco contiene regole, prendere nota delle regole e continuare con la fase 5.
5. Per rimuovere la condizione di corrispondenza SQL injection dalle regole che la utilizzano, procedere nel seguente modo:

   a. Nel pannello di navigazione, scegli Regole.
   b. Scegliere il nome di una regola che utilizza la condizione di corrispondenza SQL injection da eliminare.
   c. Nel riquadro a destra, selezionare la condizione di corrispondenza SQL injection che si desidera rimuovere dalla regola e scegliere Remove selected condition (Rimuovi condizione selezionata).
   d. Ripetere le fasi b e c per tutte le regole rimanenti che utilizzano la condizione di corrispondenza SQL injection da eliminare.
   e. Nel riquadro di navigazione scegliere SQL injection.
   f. Nel riquadro SQL injection match conditions (Condizioni di corrispondenza SQL injection), scegliere la condizione di corrispondenza SQL injection da eliminare.
6. Scegliere Delete (Elimina) per eliminare la condizione selezionata.

Utilizzo di condizioni di corrispondenza per stringa

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Se desideri consentire o bloccare le richieste Web in base alle stringe visualizzate nelle richieste, crea condizioni di corrispondenza geografica. Una condizione di corrispondenza tra stringhe identifica

la stringa da cercare e la parte di richieste Web, ad esempio un'intestazione specificata o la stringa di query, che AWS WAF Classic deve esaminare per individuare la stringa. In un secondo momento, quando crei un'ACL Web, specifichi se desideri consentire o bloccare le richieste che contengono la stringa.

Argomenti

Creazione di una condizione di corrispondenza per stringa

Quando si creano condizioni di corrispondenza tra stringhe, si specificano filtri che identificano la stringa da cercare e la parte di richieste Web che si desidera che AWS WAF Classic analizzi per quella stringa, ad esempio l'URI o la stringa di query. È possibile aggiungere più di un filtro a una condizione di corrispondenza stringa oppure è possibile creare una condizione di corrispondenza stringa separata per ogni filtro. Ecco come ogni configurazione influisce sul comportamento di AWS WAF Classic:

- Un filtro per condizione di corrispondenza della stringa: quando aggiungi condizioni di corrispondenza delle stringhe separate a una regola e aggiungi la regola a un ACL Web, le richieste Web devono soddisfare tutte le condizioni affinché AWS WAF Classic consenta o blocchi le richieste in base alle condizioni.

  Ad esempio, supponiamo che crei due condizioni. Una corrisponde alle richieste Web che contengono il valore `BadBot` nell'intestazione `User-Agent`. L'altra corrisponde alle richieste Web che contengono il valore `BadParameter` nelle stringhe di query. Quando aggiungi entrambe le condizioni alla stessa regola e aggiungi la regola a un ACL web, AWS WAF Classic consente o blocca le richieste solo quando contengono entrambi i valori.
- Più di un filtro per condizione di corrispondenza delle stringhe: quando aggiungi una condizione di corrispondenza delle stringhe che contiene più filtri a una regola e aggiungi la regola a un ACL Web, una richiesta Web deve soddisfare solo uno dei filtri nella condizione di corrispondenza delle stringhe per AWS WAF Classic per consentire o bloccare la richiesta in base a un'unica condizione.

Supponiamo di creare una condizione anziché due e che l'unica condizione contenga gli stessi due filtri dell'esempio precedente. AWS WAF La versione classica consente o blocca le richieste se sono contenute *BadBot* nell'*User-Agent*intestazione o `BadParameter` nella stringa di query.

> **Note**
>
> Quando aggiungi una condizione di corrispondenza delle stringhe a una regola, puoi anche configurare AWS WAF Classic per consentire o bloccare le richieste Web che non corrispondono ai valori della condizione.

Per creare una condizione di corrispondenza stringa

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere String and regex matching (Stringa e regex corrispondenti).
3. Scegliere Create condition (Crea condizione).
4. Specificare le impostazioni di filtro applicabili. Per ulteriori informazioni, consulta Valori da specificare durante la creazione o la modifica di condizioni di corrispondenza per stringa.
5. Scegliere Add filter (Aggiungi filtro).
6. Se si desidera aggiungere un altro filtro, ripetere le fasi 4 e 5.
7. Dopo aver aggiunto i filtri, selezionare Create (Crea).

Valori da specificare durante la creazione o la modifica di condizioni di corrispondenza per stringa

Quando crei o aggiorni una condizione di corrispondenza stringa specifichi i valori seguenti:

Nome

Immetti un nome per la condizione di corrispondenza stringa. Il nome può contenere solo caratteri alfanumerici (A - Z, a - z, 0 - 9) o i seguenti caratteri speciali: _-!"#`+*},./. Non è possibile modificare il nome di una condizione dopo averla creata.

Type

Scegliere String match (Corrispondenza stringa).

Parte della richiesta su cui applicare un filtro

Scegli la parte di ogni richiesta web a cui desideri che AWS WAF Classic controlli per verificare se la stringa specificata in Value corrisponda:

Header

Un'intestazione della richiesta specificata, ad esempio, l'intestazione `User-Agent` o `Referer`. Se scegli Header (Intestazione), specifica il nome dell'intestazione nel campo Header (Intestazione).

Metodo HTTP

Il metodo HTTP, che indica il tipo di operazione che la richiesta chiede all'origine di eseguire. CloudFront supporta i seguenti metodi: `DELETEGET`,`HEAD`, `OPTIONSPATCH`,`POST`, e`PUT`.

Stringa di query

La parte di un URL che viene visualizzata dopo un carattere `?`, se presente.

URI

Il percorso URI della richiesta, che identifica la risorsa, `/images/daily-ad.jpg` ad esempio. Ciò non include la stringa di query o i componenti del frammento dell'URI. Per informazioni, vedete Uniform Resource Identifier (URI): sintassi generica.

A meno che non venga specificata una trasformazione, un URI non viene normalizzato e viene ispezionato non appena lo AWS riceve dal client come parte della richiesta. Un valore in Transformation (Trasformazione) riformatterà l'URI come specificato.

Body

La parte di una richiesta che contiene i dati aggiuntivi da inviare al server Web come corpo della richiesta HTTP, come i dati provenienti da un modulo.

> **Note**
>
> Se scegliete Body come valore di Parte della richiesta su cui filtrare, AWS WAF Classic ispeziona solo i primi 8192 byte (8 KB). Per consentire o bloccare le richieste il cui corpo è più lungo di 8192 byte, puoi creare una condizione di vincolo di

dimensione. (AWS WAF Classic ottiene la lunghezza del corpo dalle intestazioni della richiesta.) Per ulteriori informazioni, consulta Utilizzo di condizioni per i vincoli di dimensioni.

Parametro di query singola (solo valore)

Qualsiasi parametro che hai definito come parte della stringa di query. Ad esempio, se l'URL è «www.xyz.com? UserName =abc& SalesRegion =seattle» puoi aggiungere un filtro al parametro or. UserNameSalesRegion

Se nella stringa di query vengono visualizzati parametri duplicati, i valori vengono valutati come "OR" (O). Cioè, entrambi i valori attiveranno una corrispondenza. Ad esempio, nell'URL «www.xyz.com? SalesRegion =boston& SalesRegion =seattle», «boston» o «seattle» in Value to match attiveranno una corrispondenza.

Se scegli Single query parameter (value only) (Parametro di query singola (solo valore)), sarà necessario anche specificare un valore in Query parameter name (Nome di parametro query). Questo è il parametro nella stringa di query che esaminerai, ad esempio o. UserNameSalesRegion La lunghezza massima per Query parameter name (Nome di parametro query) è 30 caratteri. Query parameter name (Nome di parametro query) non opera distinzione tra maiuscole e minuscole. Ad esempio, se si specifica UserNamecome nome del parametro Query, questo corrisponderà a tutte le varianti di UserName, come username e UserName.

Tutti i parametri di query (solo valori)

Analogamente al parametro Single query (solo valore), ma anziché controllare il valore di un singolo parametro, AWS WAF Classic esamina il valore di tutti i parametri all'interno della stringa di query per individuare il valore da abbinare. Ad esempio, se l'URL è «www.xyz.com? UserName =abc& SalesRegion =seattle» e scegli Tutti i parametri di query (solo valori), AWS WAF Classic attiverà una corrispondenza se il valore di uno dei due è specificato come Valore da abbinare. UserNameSalesRegion

Intestazione (solo quando la "Part of the request to filter on (Parte della richiesta sulla quale filtrare)" è "Header (Intestazione)")

Se hai scelto Intestazione dalla parte della richiesta per filtrare l'elenco, scegli un'intestazione dall'elenco delle intestazioni comuni o inserisci il nome di un'intestazione che desideri che AWS WAF Classic controlli.

Tipo di corrispondenza

All'interno della parte della richiesta che vuoi che AWS WAF Classic esamini, scegli dove deve apparire la stringa in Value to match per corrispondere a questo filtro:

Contiene

La stringa viene visualizzata ovunque nella parte specificata della richiesta.

Contiene parola

La parte specificata della richiesta Web deve includere Value to match (Valore per la corrispondenza) e Value to match (Valore per la corrispondenza) deve contenere solo caratteri alfanumerici o caratteri di sottolineatura (A-Z, a-z, 0-9 o _). Inoltre, Value to match (Valore per la corrispondenza) deve essere una parola, il che significa una delle seguenti opzioni:

- Value to match (Valore per la corrispondenza) corrisponde esattamente al valore della parte specificata della richiesta Web, come il valore di un'intestazione.
- Value to match (Valore per la corrispondenza) si trova all'inizio della parte specificata della richiesta Web ed è seguito da un carattere diverso da un carattere alfanumerico o un carattere di sottolineatura (_), ad esempio, `BadBot;`.
- Value to match (Valore per la corrispondenza) si trova alla fine della parte specificata della richiesta Web ed è preceduto da un carattere diverso da un carattere alfanumerico o un carattere di sottolineatura (_), ad esempio, `;BadBot`.
- Value to match (Valore per la corrispondenza) si trova al centro della parte specificata della richiesta Web ed è preceduto e seguito da caratteri diversi da caratteri alfanumerici o caratteri di sottolineatura (_), ad esempio, `-BadBot;`.

Corrispondenza esatta

La stringa e il valore della parte specificata della richiesta sono identici.

Inizia con

La stringa viene visualizzata all'inizio della parte specificata della richiesta.

Ends with

La stringa viene visualizzata alla fine della parte specificata della richiesta.

Trasformazione

Una trasformazione riformatta una richiesta web prima che AWS WAF Classic esamini la richiesta. Ciò elimina parte della formattazione insolita utilizzata dagli aggressori nelle richieste Web nel tentativo di aggirare la versione classica. AWS WAF

È possibile specificare solo un unico tipo di trasformazione del testo.

Questo è in grado di eseguire le operazioni descritte di seguito:

Nessuno

AWS WAF Classic non esegue alcuna trasformazione di testo sulla richiesta Web prima di controllarla per verificare che la stringa in Value corrisponda.

Conversione in minuscolo

AWS WAF La versione classica converte le lettere maiuscole (A-Z) in minuscole (a-z).

Decodifica HTML

AWS WAF Classic sostituisce i caratteri con codifica HTML con caratteri non codificati:

- Sostituisce `&quot;` con &
- Sostituisce ` ` con uno spazio unificatore
- Sostituisce `<` con <
- Sostituisce `>` con >
- Sostituisce i caratteri rappresentati in formato esadecimale, `&#xhhhh;`, con i caratteri corrispondenti
- Sostituisce i caratteri rappresentati in formato decimale, `&#nnnn;`, con i caratteri corrispondenti

Normalizza lo spazio vuoto

AWS WAF Classic sostituisce i seguenti caratteri con uno spazio (decimale 32):

- \f, alimentazione modulo, decimale 12
- \t, tabulazione, decimale 9
- \n, nuova riga, decimale 10
- \r, ritorno a capo, decimale 13
- \v, tabulazione verticale, decimale 11
- spazio unificatore, decimale 160

Inoltre, questa opzione sostituisce più spazi con uno spazio.

Semplificazione della riga di comando

Se sei preoccupato che gli aggressori stiano inserendo un comando da riga di comando del sistema operativo e stiano utilizzando una formattazione insolita per mascherare alcuni o tutti i comandi, utilizza questa opzione per eseguire le seguenti trasformazioni:

- Elimina i seguenti caratteri: \ " ' ^
- Eliminare gli spazi prima dei seguenti caratteri: / (
- Sostituire i seguenti caratteri con uno spazio: , ;
- Sostituire più spazi con uno spazio
- Convertire le lettere maiuscole (A-Z) in lettere minuscole (a-z)

Decodifica URL

Decodifica una richiesta con codifica URL.

Il valore è codificato con base64

Se il valore in Value to match (Valore per la corrispondenza) è codificato con base64, seleziona questa casella di controllo. Utilizza la codifica base64 per specificare i caratteri non stampabili, come le tabulazioni e gli avanzamenti riga, che gli aggressori includono nelle loro richieste.

Valore per la corrispondenza

Specificate il valore che desiderate che AWS WAF Classic cerchi nelle richieste web. La lunghezza massima è 50 byte. Se effettui la codifica base64 del valore, la lunghezza massima di 50 byte si applica al valore prima di codificarlo.

Aggiunta ed eliminazione di filtri in una condizione di corrispondenza per stringa

È possibile aggiungere a una condizione di corrispondenza per stringa o eliminare filtri. Per modificare un filtro, aggiungine uno nuovo ed elimina il precedente.

Per aggiungere o eliminare filtri in una condizione di corrispondenza stringa

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere String and regex matching (Stringa e regex corrispondenti).

3. Scegliere la condizione a aggiungere o da cui eliminare i filtri.
4. Per aggiungere filtri, procedere nel seguente modo:
   a. Scegliere Add filter (Aggiungi filtro).
   b. Specificare le impostazioni di filtro applicabili. Per ulteriori informazioni, consulta Valori da specificare durante la creazione o la modifica di condizioni di corrispondenza per stringa.
   c. Scegliere Aggiungi.
5. Per eliminare filtri, procedere nel seguente modo:
   a. Selezionare il filtro da eliminare.
   b. Scegliere Delete filter (Elimina filtro).

Eliminazione delle condizioni di corrispondenza stringa

Se desideri eliminare una condizione di corrispondenza stringa, è necessario prima eliminare tutti i filtri nella condizione e rimuovere la condizione da tutte le regole che la utilizzano, come descritto nella seguente procedura.

Per eliminare una condizione di corrispondenza stringa

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Rimuovere la condizione di corrispondenza stringa dalle regole che la utilizzano:
   a. Nel pannello di navigazione, scegli Regole.
   b. Scegliere il nome di una regola che utilizza la condizione di corrispondenza stringa da eliminare.
   c. Nel riquadro a destra, selezionare Edit rule (Modifica regola).
   d. Scegliere la X accanto alla condizione da eliminare.
   e. Scegli Aggiorna.
   f. Ripetere per tutte le regole rimanenti che utilizzano la condizione di corrispondenza stringa da eliminare.
3. Rimuovere i filtri dalla condizione da eliminare:

a. Nel riquadro di navigazione, scegliere String and regex matching (Stringa e regex corrispondenti).

b. Scegliere il nome della condizione di corrispondenza stringa da eliminare.

c. Nel riquadro a destra, scegliere la casella di controllo accanto a Filter (Filtro) per selezionare tutti i filtri.

d. Scegliere Delete filter (Elimina filtro).

4. Nel riquadro di navigazione, scegliere String and regex matching (Stringa e regex corrispondenti).
5. Nel riquadro String and regex match conditions (Condizioni di corrispondenza stringa e per regex), scegliere la condizione di corrispondenza stringa da eliminare.
6. Scegliere Delete (Elimina) per eliminare la condizione selezionata.

Utilizzo di condizioni di corrispondenza per regex

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Se desideri consentire o bloccare le richieste Web in base alle stringe che corrispondono a un modello di espressione regolare (regex) visualizzato nelle richieste, crea condizioni di corrispondenza per regex. Una condizione di corrispondenza regex è un tipo di condizione di corrispondenza tra stringhe che identifica il pattern da cercare e la parte delle richieste Web, ad esempio un'intestazione specificata o la stringa di query, che AWS WAF Classic deve esaminare per individuare il pattern. In un secondo momento, quando crei un'ACL Web, specifichi se desideri consentire o bloccare le richieste che contengono il modello.

Argomenti

- Creazione di una condizione di corrispondenza per regex
- Valori che specifichi quando crei o modifichi le condizioni di RegEx corrispondenza

- Modifica di una condizione di corrispondenza per regex

Creazione di una condizione di corrispondenza per regex

Quando si creano condizioni di corrispondenza per regex, specifichi set del modello che identificano la stringa (utilizzando un'espressione regolare) che desideri cercare. Questi set di pattern vengono quindi aggiunti ai filtri che specificano la parte di richieste Web che si desidera che AWS WAF Classic analizzi per quel set di modelli, ad esempio l'URI o la stringa di query.

È possibile aggiungere più espressioni regolari a un singolo set del modello. In questo caso, tali espressioni sono combinate con un OR (O). Cioè, una richiesta Web corrisponderà al set del modello se la parte appropriata della richiesta corrisponde a una qualsiasi delle espressioni elencate.

Quando aggiungi una condizione di corrispondenza regex a una regola, puoi anche configurare AWS WAF Classic per consentire o bloccare le richieste Web che non corrispondono ai valori della condizione.

AWS WAF Classic supporta la maggior parte delle espressioni regolari compatibili con Perl (PCRE) standard. Tuttavia, non sono supportate le seguenti:

- Backreference e sottoespressioni di acquisizione
- Asserzioni arbitrarie a larghezza nulla
- Riferimenti di subroutine e modelli ricorsivi
- Modelli condizionali
- Verbi di controllo di backtracking
- La direttiva\C a byte singolo
- La direttiva \R di corrispondenza nuova riga
- L'inizio \K della direttiva di reimpostazione della corrispondenza
- Callout e codice incorporato
- Raggruppamento atomico e quantificatori possessivi

Per creare una condizione di corrispondenza regex

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.

2. Nel riquadro di navigazione, scegliere String and regex matching (Stringa e regex corrispondenti).
3. Scegliere Create condition (Crea condizione).
4. Specificare le impostazioni di filtro applicabili. Per ulteriori informazioni, consulta Valori che specifichi quando crei o modifichi le condizioni di RegEx corrispondenza.
5. Scegliere Create pattern set and add filter (Crea set del modello e aggiungi filtro) (se è stato creato un nuovo set del modello) o Add filter (Aggiungi filtro) se è stato utilizzato un set del modello esistente.
6. Scegli Crea.

Valori che specifichi quando crei o modifichi le condizioni di RegEx corrispondenza

Quando crei o aggiorni una condizione di corrispondenza per regex specifichi i valori seguenti:

Nome

Immetti un nome per la condizione di corrispondenza per regex. Il nome può contenere solo caratteri alfanumerici (A - Z, a - z, 0 - 9) o i seguenti caratteri speciali: _-!"#`+*},./. Non è possibile modificare il nome di una condizione dopo averla creata.

Type

Scegliere Regex match (Corrispondenza regex).

Parte della richiesta su cui applicare un filtro

Scegliete la parte di ogni richiesta web a cui desiderate che AWS WAF Classic esamini per verificare la corrispondenza del modello specificato in Valore:

Header

Un'intestazione della richiesta specificata, ad esempio, l'intestazione `User-Agent` o `Referer`. Se scegli Header (Intestazione), specifica il nome dell'intestazione nel campo Header (Intestazione).

Metodo HTTP

Il metodo HTTP, che indica il tipo di operazione che la richiesta chiede all'origine di eseguire. CloudFront supporta i seguenti metodi: `DELETEGET`,`HEAD`, `OPTIONSPATCH`,`POST`, e`PUT`.

Stringa di query

La parte di un URL che viene visualizzata dopo un carattere ?, se presente.

URI

Il percorso URI della richiesta, che identifica la risorsa, `/images/daily-ad.jpg` ad esempio. Ciò non include la stringa di query o i componenti del frammento dell'URI. Per informazioni, vedete Uniform Resource Identifier (URI): sintassi generica.

A meno che non venga specificata una trasformazione, un URI non viene normalizzato e viene ispezionato non appena lo AWS riceve dal client come parte della richiesta. Un valore in Transformation (Trasformazione) riformatterà l'URI come specificato.

Body

La parte di una richiesta che contiene i dati aggiuntivi da inviare al server Web come corpo della richiesta HTTP, come i dati provenienti da un modulo.

> **Note**
>
> Se scegliete Body come valore di Parte della richiesta su cui filtrare, AWS WAF Classic ispeziona solo i primi 8192 byte (8 KB). Per consentire o bloccare le richieste il cui corpo è più lungo di 8192 byte, puoi creare una condizione di vincolo di dimensione. (AWS WAF Classic ottiene la lunghezza del corpo dalle intestazioni della richiesta.) Per ulteriori informazioni, consulta Utilizzo di condizioni per i vincoli di dimensioni.

Parametro di query singola (solo valore)

Qualsiasi parametro che hai definito come parte della stringa di query. Ad esempio, se l'URL è «www.xyz.com? UserName =abc& SalesRegion =seattle» puoi aggiungere un filtro al parametro or. UserNameSalesRegion

Se nella stringa di query vengono visualizzati parametri duplicati, i valori vengono valutati come "OR" (O). Cioè, entrambi i valori attiveranno una corrispondenza. Ad esempio, nell'URL «www.xyz.com? SalesRegion =boston& SalesRegion =seattle», un pattern che corrisponde a «boston» o «seattle» in Value to match attiverà una corrispondenza.

Se scegli Single query parameter (value only) (Parametro di query singola (solo valore)), sarà necessario anche specificare un valore in Query parameter name (Nome di parametro

query). Questo è il parametro nella stringa di query che esaminerai, ad esempio o. UserNameSalesRegion La lunghezza massima per Query parameter name (Nome di parametro query) è 30 caratteri. Query parameter name (Nome di parametro query) non opera distinzione tra maiuscole e minuscole. Ad esempio, se si specifica UserNamecome nome del parametro Query, questo corrisponderà a tutte le varianti di UserName, come username e UserName.

Tutti i parametri di query (solo valori)

Analogamente al parametro Single query (solo valore), ma anziché controllare il valore di un singolo parametro, AWS WAF Classic esamina il valore di tutti i parametri all'interno della stringa di query per individuare il modello specificato in Valore da abbinare. Ad esempio, nell'URL «www.xyz.com? UserName =abc& SalesRegion =seattle», un pattern in Value to match che corrisponde al valore in o attiverà una corrispondenza. UserNameSalesRegion

Intestazione (solo quando la "Part of the request to filter on (Parte della richiesta sulla quale filtrare)" è "Header (Intestazione)")

Se hai scelto Intestazione dalla parte della richiesta per filtrare l'elenco, scegli un'intestazione dall'elenco delle intestazioni comuni o inserisci il nome di un'intestazione che desideri che Classic controlli. AWS WAF

Trasformazione

Una trasformazione riformatta una richiesta web prima che Classic esamini la richiesta. AWS WAF Ciò elimina parte della formattazione insolita utilizzata dagli aggressori nelle richieste Web nel tentativo di aggirare la versione classica. AWS WAF

È possibile specificare solo un unico tipo di trasformazione del testo.

Questo è in grado di eseguire le operazioni descritte di seguito:

Nessuno

AWS WAF Classic non esegue alcuna trasformazione di testo sulla richiesta Web prima di controllarla per verificare che la stringa in Value corrisponda.

Conversione in minuscolo

AWS WAF La versione classica converte le lettere maiuscole (A-Z) in minuscole (a-z).

Decodifica HTML

AWS WAF Classic sostituisce i caratteri con codifica HTML con caratteri non codificati:

- Sostituisce " con &
- Sostituisce   con uno spazio unificatore
- Sostituisce < con <
- Sostituisce > con >
- Sostituisce i caratteri rappresentati in formato esadecimale, &#xhhhh;, con i caratteri corrispondenti
- Sostituisce i caratteri rappresentati in formato decimale, &#nnnn;, con i caratteri corrispondenti

Normalizza lo spazio vuoto

AWS WAF Classic sostituisce i seguenti caratteri con uno spazio (decimale 32):

- \f, alimentazione modulo, decimale 12
- \t, tabulazione, decimale 9
- \n, nuova riga, decimale 10
- \r, ritorno a capo, decimale 13
- \v, tabulazione verticale, decimale 11
- spazio unificatore, decimale 160

Inoltre, questa opzione sostituisce più spazi con uno spazio.

Semplificazione della riga di comando

Se sei preoccupato che gli aggressori stiano inserendo un comando da riga di comando del sistema operativo e stiano utilizzando una formattazione insolita per mascherare alcuni o tutti i comandi, utilizza questa opzione per eseguire le seguenti trasformazioni:

- Elimina i seguenti caratteri: \ " ' ^
- Eliminare gli spazi prima dei seguenti caratteri: / (
- Sostituire i seguenti caratteri con uno spazio: , ;
- Sostituire più spazi con uno spazio
- Convertire le lettere maiuscole (A-Z) in lettere minuscole (a-z)

Decodifica URL

Decodifica una richiesta con codifica URL.

Modello regex che corrisponde alla richiesta

È possibile scegliere un set del modello esistente o crearne uno nuovo. Se ne crei uno nuovo, specifica quanto segue:

Nuovo nome del set del modello

Immettete un nome, quindi specificate lo schema regex che desiderate che AWS WAF Classic cerchi.

Se aggiungi più espressioni regolari a un set del modello, tali espressioni sono combinate con un OR (O). Cioè, una richiesta Web corrisponderà al set del modello se la parte appropriata della richiesta corrisponde a una qualsiasi delle espressioni elencate.

La lunghezza massima di Value to match (Valore per la corrispondenza) è di 70 caratteri.

Modifica di una condizione di corrispondenza per regex

È possibile apportare le seguenti modifiche a una condizione di corrispondenza per regex esistente:

- Eliminare un modello da un set del modello esistente
- Aggiungere un modello a un set del modello esistente
- Eliminare un filtro in una condizione di corrispondenza per regex esistente
- Aggiungi un filtro a una condizione di corrispondenza regex esistente (puoi avere solo un filtro in una condizione di corrispondenza regex. Pertanto, per aggiungere un filtro, è necessario prima eliminare il filtro esistente.)
- Eliminare una condizione di corrispondenza per regex esistente

> **Note**
>
> Non è possibile aggiungere o eliminare un set del modello da un filtro esistente. È necessario modificare il set del modello o eliminare il filtro e creare un nuovo filtro con un nuovo set del modello.

Per eliminare un modello da un set del modello esistente

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.

2. Nel riquadro di navigazione, scegliere String and regex matching (Stringa e regex corrispondenti).
3. Scegliere View regex pattern sets (Visualizza set del modello regex).
4. Scegliere il nome del set del modello da modificare.
5. Scegli Modifica.
6. Scegliere la X accanto al modello da eliminare.
7. Selezionare Salva.

Per aggiungere un modello a un set del modello esistente

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere String and regex matching (Stringa e regex corrispondenti).
3. Scegliere View regex pattern sets (Visualizza set del modello regex).
4. Scegliere il nome del set del modello da modificare.
5. Scegli Modifica.
6. Immettere un nuovo modello regex.
7. Scegliere il + accanto al nuovo modello.
8. Selezionare Salva.

Per eliminare un filtro da una condizione di corrispondenza per regex esistente

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere String and regex matching (Stringa e regex corrispondenti).
3. Scegliere il nome della condizione con il filtro da eliminare.

4. Scegliere la casella accanto al filtro da eliminare.
5. Scegli Delete filter (Elimina filtro).

Per eliminare una condizione di corrispondenza per regex

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Eliminare il filtro dalla condizione regex. Per istruzioni su come eseguire questa operazione, consulta Per eliminare un filtro da una condizione di corrispondenza per regex esistente.
3. Rimuovere la condizione di corrispondenza per regex dalle regole che la utilizzano:
   a. Nel pannello di navigazione, scegli Regole.
   b. Scegliere il nome di una regola che utilizza la condizione di corrispondenza per regex da eliminare.
   c. Nel riquadro a destra, selezionare Edit rule (Modifica regola).
   d. Scegliere la X accanto alla condizione da eliminare.
   e. Scegli Aggiorna.
   f. Ripetere per tutte le regole rimanenti che utilizzano la condizione di corrispondenza per regex da eliminare.
4. Nel riquadro di navigazione, scegliere String and regex matching (Stringa e regex corrispondenti).
5. Selezionare il pulsante accanto alla condizione da eliminare.
6. Scegli Elimina.

Per aggiungere o modificare un filtro in una condizione di corrispondenza per regex esistente

È possibile disporre di un solo filtro in una condizione corrispondenza per regex. Se si desidera aggiungere o modificare il filtro, è necessario prima eliminare il filtro esistente.

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.

2. Eliminare il filtro dalla condizione regex da modificare. Per istruzioni su come eseguire questa operazione, consulta Per eliminare un filtro da una condizione di corrispondenza per regex esistente.
3. Nel riquadro di navigazione, scegliere String and regex matching (Stringa e regex corrispondenti).
4. Scegliere il nome della condizione da modificare.
5. Scegliere Add filter (Aggiungi filtro).
6. Inserire i valori appropriati per il nuovo filtro e scegliere Add (Aggiungi).

Utilizzo delle regole

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Le regole ti consentono di indirizzare con precisione le richieste web che vuoi che AWS WAF Classic consenta o blocchi specificando le condizioni esatte che vuoi che AWS WAF Classic tenga d'occhio. Ad esempio, AWS WAF Classic può controllare gli indirizzi IP da cui provengono le richieste, le stringhe che le richieste contengono e dove appaiono le stringhe e se le richieste sembrano contenere codice SQL dannoso.

Argomenti

- Creazione di una regola e aggiunta di condizioni
- Aggiunta e rimozione di condizioni in una regola
- Eliminazione di una regola
- Marketplace AWS gruppi di regole

Creazione di una regola e aggiunta di condizioni

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Se aggiungi più di una condizione a una regola, una richiesta web deve soddisfare tutte le condizioni affinché AWS WAF Classic consenta o blocchi le richieste basate su quella regola.

Per creare una regola e aggiungere condizioni

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel pannello di navigazione, scegli Regole.
3. Scegli Crea regola.
4. Immetti uno dei seguenti valori:

   Nome

   Inserire un nome.

   CloudWatch nome della metrica

   Inserisci un nome per la CloudWatch metrica che AWS WAF Classic creerà e assocerà alla regola. Il nome può contenere solo caratteri alfanumerici (A - Z, a - z, 0-9), con lunghezza massima di 128 e lunghezza minima di 1. Non può contenere spazi bianchi o nomi di metriche riservati a AWS WAF Classic, inclusi «All» e «Default_Action.

   Tipo di regola

   Scegliere `Regular rule` o `Rate-based rule`. Le regole basate sulla frequenza sono identiche alle regole normali, ma tengono conto anche del numero di richieste che arrivano da

un indirizzo IP in un periodo di cinque minuti. Per ulteriori informazioni su questi tipi di regole, consulta Come funziona AWS WAF Classic.

Limite frequenza

Per una regola basata sulla frequenza, immetti il numero massimo di richieste da consentire in un periodo di cinque minuti da un indirizzo IP che soddisfa le condizioni della regola. Il limite di aliquota deve essere di almeno 100.

Puoi specificare solo un limite di frequenza o un limite di frequenza e condizioni. Se si specifica solo un limite di velocità, imposta il limite su AWS WAF tutti gli indirizzi IP. Se si specificano un limite di velocità e delle condizioni AWS WAF , impone il limite agli indirizzi IP che soddisfano le condizioni.

Quando un indirizzo IP raggiunge la soglia limite di velocità, AWS WAF applica l'azione assegnata (blocco o conteggio) il più rapidamente possibile, di solito entro 30 secondi. Una volta completata l'azione, se trascorrono cinque minuti senza che l'indirizzo IP richieda alcuna richiesta, AWS WAF azzera il contatore.

5. Per aggiungere una condizione alla regola, specificare i seguenti valori:

Quando una richiesta include/esclude

Se desideri che AWS WAF Classic consenta o blocchi le richieste in base ai filtri di una determinata condizione, scegli Sì. Ad esempio, se una condizione di corrispondenza IP include l'intervallo di indirizzi IP 192.0.2.0/24 e desideri che AWS WAF Classic consenta o blocchi le richieste provenienti da tali indirizzi IP, scegli Sì.

Se desideri che AWS WAF Classic consenta o blocchi le richieste in base all'inverso dei filtri in una condizione, scegli No. Ad esempio, se una condizione di corrispondenza IP include l'intervallo di indirizzi IP 192.0.2.0/24 e desideri che AWS WAF Classic consenta o blocchi le richieste che non provengono da tali indirizzi IP, scegli No.

corrispondenza a/origine da

Scegliere il tipo di condizione da aggiungere alla regola:

- Condizioni di corrispondenza dello scripting tra siti: scegli abbina almeno uno dei filtri nella condizione di corrispondenza dello scripting tra siti
- Condizioni di corrispondenza IP: scegli l'origine da un indirizzo IP in
- Condizioni di corrispondenza geografica: scegli la provenienza da una posizione geografica in

- Condizioni di vincolo di dimensione: scegli abbina almeno uno dei filtri nella condizione di vincolo di dimensione
- Condizioni di corrispondenza di iniezione SQL: scegli abbina almeno uno dei filtri nella condizione di corrispondenza di iniezione SQL
- Condizioni di corrispondenza delle stringhe: scegli abbina almeno uno dei filtri nella condizione di corrispondenza delle stringhe
- Condizioni di corrispondenza delle espressioni regolari: scegli abbina almeno uno dei filtri nella condizione di corrispondenza regex

nome della condizione

Scegliere la condizione da aggiungere alla regola. L'elenco visualizza solo le condizioni del tipo scelto nella fase precedente.

6. Per aggiungere un'altra condizione alla regola, scegliere Add another condition (Aggiungi un'altra condizione) e ripetere le fasi 4 e 5. Tieni presente quanto segue:
   - Se aggiungi più di una condizione, una richiesta web deve soddisfare almeno un filtro in ogni condizione affinché AWS WAF Classic consenta o blocchi le richieste basate su quella regola
   - Se aggiungi due condizioni di corrispondenza IP alla stessa regola, AWS WAF Classic consentirà o bloccherà solo le richieste che provengono da indirizzi IP che compaiono in entrambe le condizioni di corrispondenza IP
7. Dopo aver aggiunto le condizioni, selezionare Create (Crea).

Aggiunta e rimozione di condizioni in una regola

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

È possibile modificare una regola aggiungendo o rimuovendo le condizioni.

Per aggiungere o rimuovere le condizioni in una regola

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel pannello di navigazione, scegli Regole.
3. Scegliere il nome della regola in cui si desidera aggiungere o rimuovere le condizioni.
4. Scegli Aggiungi regola.
5. Per aggiungere una condizione, scegliere Add condition (Aggiungi condizione) e specificare i seguenti valori:

   Quando una richiesta include/esclude

   Se desideri che AWS WAF Classic consenta o blocchi le richieste in base ai filtri in una condizione, ad esempio le richieste Web che provengono dall'intervallo di indirizzi IP 192.0.2.0/24, scegli does.

   Se desideri che AWS WAF Classic consenta o blocchi le richieste in base all'inverso dei filtri in una condizione, scegli No. Ad esempio, se una condizione di corrispondenza IP include l'intervallo di indirizzi IP 192.0.2.0/24 e desideri che AWS WAF Classic consenta o blocchi le richieste che non provengono da tali indirizzi IP, scegli No.

   corrispondenza a/origine da

   Scegliere il tipo di condizione da aggiungere alla regola:

   - Condizioni di corrispondenza dello scripting tra siti: scegli abbina almeno uno dei filtri nella condizione di corrispondenza dello scripting tra siti
   - Condizioni di corrispondenza IP: scegli l'origine da un indirizzo IP in
   - Condizioni di corrispondenza geografica: scegli la provenienza da una posizione geografica in
   - Condizioni di vincolo di dimensione: scegli abbina almeno uno dei filtri nella condizione di vincolo di dimensione
   - Condizioni di corrispondenza di iniezione SQL: scegli abbina almeno uno dei filtri nella condizione di corrispondenza di iniezione SQL
   - Condizioni di corrispondenza delle stringhe: scegli abbina almeno uno dei filtri nella condizione di corrispondenza delle stringhe

- Condizioni di corrispondenza delle espressioni regolari: scegli abbina almeno uno dei filtri nella condizione di corrispondenza regex

nome della condizione

Scegliere la condizione da aggiungere alla regola. L'elenco visualizza solo le condizioni del tipo scelto nella fase precedente.

6. Per rimuovere una condizione, selezionare la X a destra del nome della condizione.
7. Scegli Aggiorna.

Eliminazione di una regola

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Se desideri eliminare una regola, è necessario prima rimuovere la regola dalle ACL Web che la utilizzano e rimuovere le condizioni incluse nella regola.

Per eliminare una regola

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Per rimuovere la regola dagli ACL Web che la utilizzano, procedi come segue per ciascuno degli ACL Web:

   a. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).
   b. Scegliere il nome di un'ACL Web che utilizza la regola da eliminare.
   c. Scegliere la scheda Rules (Regole).
   d. Scegliere Edit web ACL (Modifica ACL Web).

e. Scegli la X a destra della regola che desideri eliminare, quindi scegli Aggiorna.

3. Nel pannello di navigazione, scegli Regole.
4. Selezionare il nome della regola da eliminare.
5. Scegli Delete (Elimina).

Marketplace AWS gruppi di regole

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

AWS WAF Classic fornisce gruppi di Marketplace AWS regole per aiutarti a proteggere le tue risorse. Marketplace AWS i gruppi di regole sono raccolte di ready-to-use regole predefinite, scritte e aggiornate da AWS aziende AWS partner.

Alcuni gruppi di Marketplace AWS regole sono progettati per aiutare a proteggere tipi specifici di applicazioni Web come WordPress Joomla o PHP. Altri gruppi di Marketplace AWS regole offrono un'ampia protezione contro le minacce note o le vulnerabilità più comuni delle applicazioni Web, come quelle elencate nella Top 10 di OWASP.

Puoi installare un singolo gruppo di Marketplace AWS regole dal tuo AWS partner preferito e puoi anche aggiungere regole AWS WAF Classic personalizzate per una maggiore protezione. Se sei soggetto alla conformità normativa come PCI o HIPAA, potresti essere in grado di utilizzare gruppi di Marketplace AWS regole per soddisfare i requisiti del firewall delle applicazioni Web.

Marketplace AWS i gruppi di regole sono disponibili senza contratti a lungo termine e senza impegni minimi. Al momento della sottoscrizione a un gruppo di regole, vengono addebitate una tariffa mensile (ripartita proporzionalmente nell'ora), nonché le tariffe continue basate sul volume delle richieste. Per ulteriori informazioni, consulta la sezione Prezzi AWS WAF classici e la descrizione di ciascun gruppo di Marketplace AWS regole su Marketplace AWS.

Aggiornamenti automatici

Rimanere aggiornati sul panorama delle minacce in continua evoluzione può richiedere molto tempo e denaro. Marketplace AWS i gruppi di regole possono farti risparmiare tempo quando implementi e usi AWS WAF Classic. Un altro vantaggio è rappresentato dal fatto che AWS i nostri AWS partner aggiornano automaticamente i gruppi di Marketplace AWS regole quando emergono nuove vulnerabilità e minacce.

Molti dei nostri partner vengono informati delle nuove vulnerabilità prima delle comunicazioni pubbliche. Possono aggiornare i loro gruppi di regole e distribuirli ancora prima che una nuova minaccia sia ampiamente nota. Molti dispongono anche di team di ricerca sulle minacce per indagare e analizzare le minacce più recenti al fine di scrivere le regole più rilevanti.

Accesso alle regole in un gruppo di Marketplace AWS regole

Ogni gruppo di Marketplace AWS regole fornisce una descrizione completa dei tipi di attacchi e vulnerabilità da cui è progettato per proteggere. Per proteggere la proprietà intellettuale dei fornitori del gruppo di regole, non è possibile visualizzare le singole regole all'interno di un gruppo di regole. Questa restrizione consente anche di impedire agli utenti malintenzionati di progettare minacce che eludano in modo specifico le regole pubblicate.

Poiché non è possibile visualizzare le singole regole in un Marketplace AWS gruppo di regole, non è possibile modificare alcuna Marketplace AWS regola in un gruppo di regole. Tuttavia, è possibile escludere da un gruppo di regole delle regole specifiche. Questa operazione viene chiamata "eccezione dei gruppi di regole". L'esclusione delle regole non le rimuove. Piuttosto, modifica l'operazione delle regole in `COUNT`. Pertanto, le richieste che corrispondono a una regola esclusa sono conteggiate, ma non bloccate. Riceverai i parametri COUNT per ogni regola esclusa.

L'esclusione delle regole può essere utile nella risoluzione dei problemi dei gruppi di regole che bloccano in modo imprevisto il traffico (falsi positivi). Una tecnica per la risoluzione dei problemi è quella di identificare la regola specifica nel gruppo di regole che sta bloccando il traffico desiderato e quindi disabilitare (escludere) tale regola.

Oltre a escludere regole specifiche, è possibile perfezionare la protezione abilitando o disabilitando interi gruppi di regole oppure scegliendo l'operazione che il gruppo di regole deve eseguire. Per ulteriori informazioni, consulta Utilizzo dei gruppi di Marketplace AWS regole.

Quote

È possibile abilitare solo un gruppo di Marketplace AWS regole. È inoltre possibile abilitare un gruppo di regole personalizzato creato utilizzando AWS Firewall Manager. Questi gruppi di regole vengono

conteggiati per la quota massima di 10 regole per ACL Web. Pertanto, è possibile avere un gruppo di Marketplace AWS regole, un gruppo di regole personalizzato e fino a otto regole personalizzate in un unico ACL Web.

Prezzi

Per informazioni sui prezzi per gruppi di Marketplace AWS regole, consulta la sezione Prezzi AWS WAF classici e la descrizione di ogni gruppo di Marketplace AWS regole su Marketplace AWS.

Utilizzo dei gruppi di Marketplace AWS regole

È possibile sottoscrivere e annullare l'iscrizione ai gruppi di Marketplace AWS regole sulla console AWS WAF Classic. È anche possibile escludere da un gruppo di regole delle regole specifiche.

Per sottoscrivere e utilizzare un gruppo di Marketplace AWS regole

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, selezionare Marketplace.
3. Nella sezione Available marketplace products (Prodotti Marketplace disponibili), scegliere il nome di un gruppo di regole per visualizzare dettagli e informazioni sui prezzi.
4. Se si desidera effettuare la sottoscrizione al gruppo di regole, scegliere Continue (Continua).

   > **Note**
   >
   > Se non si desidera effettuare la sottoscrizione a questo gruppo di regole, è sufficiente chiudere questa pagina nel browser.
5. Scegliere Set up your account (Configura account).
6. Aggiungere il gruppo di regole a un'ACL Web, proprio come se si dovesse aggiungere una singola regola. Per ulteriori informazioni, consulta Creazione di un'ACL Web o Modifica di un'ACL Web.

   > **Note**
   >
   > Quando si aggiunge un gruppo di regole a un'ACL Web, l'operazione che viene impostata per il gruppo di regole (No override (Non sostituire) o Override to count

(Sostituisci per contare)) è denominata operazione di sostituzione del gruppo di regole. Per ulteriori informazioni, consulta Sostituzione del gruppo di regole.

Per annullare l'iscrizione a un gruppo di Marketplace AWS regole

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Rimuovere il gruppo di regole da tutte le ACL Web. Per ulteriori informazioni, consulta Modifica di un'ACL Web.
3. Nel riquadro di navigazione, selezionare Marketplace.
4. Scegliere Manage your subscriptions (Gestisci sottoscrizioni).
5. Scegliere Cancel subscription (Annulla sottoscrizione) accanto al nome del gruppo di regole di cui si desidera annullare la sottoscrizione.
6. Scegliere Yes, cancel subscription (Sì, annulla sottoscrizione).

Per escludere una regola da un gruppo di regole (eccezione del gruppo di regole)

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Se non è già abilitato, abilita la registrazione AWS WAF classica. Per ulteriori informazioni, consulta Registrazione informazioni di traffico ACL Web. Utilizza i log AWS WAF classici per identificare gli ID delle regole che desideri escludere. Queste sono in genere regole che bloccano richieste legittime.
3. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).
4. Scegliere l'ACL Web che si desidera modificare. Si apre una pagina con i dettagli dell'ACL Web nel riquadro a destra.

> **Note**
>
> Il gruppo di regole che desideri modificare deve essere associato a una ACL Web prima di poter escludere una regola dal gruppo.

5. Nella scheda Rules (Regole) nel riquadro a destra, scegliere Edit web ACL (Modifica ACL Web).
6. Nella sezione Rule group exceptions (Eccezioni gruppo di regole) espandi il gruppo di regole che desideri modificare.
7. Scegli la X accanto alla regola che desideri escludere. È possibile identificare l'ID corretto della regola utilizzando i log AWS WAF classici.
8. Scegli Aggiorna.

L'esclusione delle regole non le rimuove dal gruppo di regole. Piuttosto, modifica l'operazione delle regole in `COUNT`. Pertanto, le richieste che corrispondono a una regola esclusa sono conteggiate, ma non bloccate. Riceverai i parametri `COUNT` per ogni regola esclusa.

> **Note**
>
> È possibile utilizzare la stessa procedura per escludere regole da gruppi di regole personalizzate creati in AWS Firewall Manager. Tuttavia, invece di escludere una regola da un gruppo di regole personalizzate utilizzando queste fasi, puoi anche semplicemente modificare un gruppo di regole personalizzate utilizzando le fasi descritte in Aggiungere ed eliminare regole da un gruppo di regole AWS WAF classico.

Sostituzione del gruppo di regole

Marketplace AWS i gruppi di regole hanno due azioni possibili: No override e Override to count. Se si desidera verificare il gruppo di regole, impostare l'operazione su Override to count (Sostituisci per contare). Questa operazione del gruppo di regole sovrascrive qualsiasi operazione di blocco specificata dalle singole regole contenute nel gruppo. Vale a dire, se l'operazione del gruppo di regole è impostata su Override to count (Sostituisci per contare), anziché potenzialmente bloccare le richieste corrispondenti in base all'operazione delle singole regole all'interno del gruppo, tali richieste verranno conteggiate. Al contrario, se si imposta l'operazione del gruppo di regole su No override (Non sostituire), verranno usate le operazioni delle singole regole all'interno del gruppo.

Risoluzione dei problemi relativi ai gruppi di regole Marketplace AWS

Se scopri che un gruppo di Marketplace AWS regole sta bloccando il traffico legittimo, procedi nel seguente modo.

Per risolvere i problemi relativi a un gruppo di regole Marketplace AWS

1. Escludere regole specifiche che bloccano il traffico legittimo. Puoi identificare quali regole bloccano quali richieste utilizzando i log AWS WAF classici. Per ulteriori informazioni sull'esclusione delle regole, consulta Per escludere una regola da un gruppo di regole (eccezione del gruppo di regole).
2. Se l'esclusione di regole specifiche non risolve il problema, è possibile modificare l'azione per il gruppo di Marketplace AWS regole da No override a Override per conteggiare. Ciò consente il transito della richiesta Web, indipendentemente dalle singole operazioni delle regole all'interno del gruppo di regole. Questo ti fornisce anche i CloudWatch parametri di Amazon per il gruppo di regole.
3. Dopo aver impostato l'azione del gruppo di Marketplace AWS regole su Override to count, contatta il team di assistenza clienti del fornitore del gruppo di regole per risolvere ulteriormente il problema. Per informazioni di contatto, consulta l'elenco dei gruppi di regole nelle pagine di elenco dei prodotti su Marketplace AWS.

Come contattare il supporto clienti

Per problemi con AWS WAF Classic o con un gruppo di regole gestito da AWS, contatta. AWS Support Per problemi con un gruppo di regole gestito da un AWS partner, contatta il team di assistenza clienti di quel partner. Per trovare le informazioni di contatto del partner, consulta l'elenco del partner su Marketplace AWS.

Creazione e vendita di gruppi di Marketplace AWS regole

Se desideri vendere gruppi di Marketplace AWS regole su Marketplace AWS, consulta Come vendere il tuo software su Marketplace AWS.

Utilizzo delle ACL Web

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e

non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
Per la versione più recente di AWS WAF, vedi. AWS WAF

Quando si aggiungono regole a un ACL Web, si specifica se si desidera che AWS WAF Classic consenta o blocchi le richieste in base alle condizioni delle regole. Se aggiungi più di una regola a un ACL web, AWS WAF Classic valuta ogni richiesta rispetto alle regole nell'ordine in cui le elenchi nell'ACL web. Quando una richiesta web soddisfa tutte le condizioni di una regola, AWS WAF Classic esegue immediatamente l'azione corrispondente (consentire o bloccare) e non valuta la richiesta rispetto alle regole rimanenti nell'ACL web, se presenti.

Se una richiesta Web non corrisponde a nessuna delle regole di un ACL Web, AWS WAF Classic esegue l'azione predefinita specificata per l'ACL Web. Per ulteriori informazioni, consulta Decisione dell'operazione predefinita per un'ACL Web.

Se desideri testare una regola prima di iniziare a utilizzarla per consentire o bloccare le richieste, puoi configurare AWS WAF Classic per contare le richieste Web che soddisfano le condizioni della regola. Per ulteriori informazioni, consulta Test delle ACL Web.

Argomenti

Decisione dell'operazione predefinita per un'ACL Web

Note

Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.

Per la versione più recente di AWS WAF, vedi. AWS WAF

Quando create e configurate un ACL Web, la prima e più importante decisione da prendere è se l'azione predefinita debba essere quella di consentire le richieste Web nella AWS WAF versione classica o di bloccare le richieste Web. L'azione predefinita indica cosa volete che AWS WAF Classic faccia dopo aver esaminato una richiesta web per tutte le condizioni specificate e la richiesta web non soddisfa nessuna di queste condizioni:

- Consenti: se desideri consentire alla maggior parte degli utenti di accedere al tuo sito Web, ma desideri bloccare l'accesso agli aggressori le cui richieste provengono da indirizzi IP specifici o le cui richieste sembrano contenere codice SQL dannoso o valori specifici, scegli Consenti come azione predefinita.
- Blocca: se desideri impedire alla maggior parte dei potenziali utenti di accedere al tuo sito Web, ma desideri consentire l'accesso agli utenti le cui richieste provengono da indirizzi IP specifici o le cui richieste contengono valori specifici, scegli Blocca per l'azione predefinita.

Molte decisioni prese dopo aver deciso un'operazione predefinita dipendono dal fatto che desideri consentire o bloccare la maggior parte delle richieste Web. Ad esempio, se desideri consentire la maggior parte delle richieste , le condizioni di corrispondenza che crei in generale dovrebbero specificare le richieste Web che desideri bloccare, come ad esempio:

- Richieste che hanno origine da indirizzi IP che stanno effettuando un numero irragionevole di richieste
- Richieste che hanno origine da paesi nei quali non operi o che sono frequenti fonti di attacchi
- Richieste che includono valori falsi nell'intestazione User-Agent
- Richieste che sembrano includere codice SQL dannoso

Creazione di un'ACL Web

Note

Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.

Per la versione più recente di AWS WAF, vedi. AWS WAF

Per creare un'ACL Web

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Se è la prima volta che usi la AWS WAF versione classica, scegli Vai alla AWS WAF versione classica e quindi Configura Web ACL. Se hai già utilizzato la AWS WAF versione classica, scegli Web ACL nel riquadro di navigazione, quindi scegli Crea ACL web.
3. Per il nome Web ACL, inserisci un nome.

   > **Note**
   >
   > Non è possibile modificare il nome dopo aver creato l'ACL Web.
4. Per il nome della CloudWatch metrica, modifica il nome predefinito, se applicabile. Il nome può contenere solo caratteri alfanumerici (A - Z, a - z, 0-9), con lunghezza massima di 128 e lunghezza minima di 1. Non può contenere spazi bianchi o nomi di metriche riservati a AWS WAF Classic, inclusi «All» e «Default_Action».

   > **Note**
   >
   > Non è possibile modificare il nome dopo aver creato l'ACL Web.
5. In Region (Regione), scegliere una Regione.
6. Per AWS risorsa, scegliete la risorsa che desiderate associare a questo ACL Web, quindi scegliete Avanti.
7. Se hai già creato le condizioni che desideri che AWS WAF Classic utilizzi per esaminare le tue richieste web, scegli Avanti e procedi con il passaggio successivo.

   Se non sono ancora state create condizioni, farlo ora. Per ulteriori informazioni, consulta i seguenti argomenti:

   - Utilizzo di condizioni di corrispondenza Cross-site scripting
   - Utilizzo di condizioni di corrispondenza IP

- Utilizzo di condizioni di corrispondenza geografica
- Utilizzo di condizioni per i vincoli di dimensioni
- Utilizzo di condizioni di corrispondenza SQL injection
- Utilizzo di condizioni di corrispondenza per stringa
- Utilizzo di condizioni di corrispondenza per regex

8. Se hai già creato le regole o i gruppi di regole (o ti sei iscritto a un gruppo di Marketplace AWS regole) che desideri aggiungere a questo ACL web, aggiungi le regole all'ACL web:

   a. Nell'elenco Rules (Regole), scegliere una regola.

   b. Scegliere Add rule to web ACL (Aggiungi regola all'ACL Web).

   c. Ripetere le fasi a e b fino a quando non sono state aggiunte tutte le regole da aggiungere a questa ACL Web.

   d. Andare alla fase 10.

9. Se non sono ancora state create regole, è possibile aggiungere le regole ora:

   a. Scegli Crea regola.

   b. Immetti uno dei seguenti valori:

      Nome

      Inserire un nome.

      CloudWatch nome della metrica

      Inserisci un nome per la CloudWatch metrica che AWS WAF Classic creerà e assocerà alla regola. Il nome può contenere solo caratteri alfanumerici (A - Z, a - z, 0-9), con lunghezza massima di 128 e lunghezza minima di 1. Non può contenere spazi bianchi o nomi di metriche riservati a AWS WAF Classic, inclusi «All» e «Default_Action».

      > **Note**
      >
      > Non è possibile modificare il nome del parametro dopo aver creato la regola.

   c. Per aggiungere una condizione alla regola, specificare i seguenti valori:

Quando una richiesta include/esclude

Se desideri che AWS WAF Classic consenta o blocchi le richieste in base ai filtri in una condizione, ad esempio le richieste Web che provengono dall'intervallo di indirizzi IP 192.0.2.0/24, scegli does.

Se desideri che AWS WAF Classic consenta o blocchi le richieste in base all'inverso dei filtri in una condizione, scegli No. Ad esempio, se una condizione di corrispondenza IP include l'intervallo di indirizzi IP 192.0.2.0/24 e desideri che AWS WAF Classic consenta o blocchi le richieste che non provengono da tali indirizzi IP, scegli No.

corrispondenza a/origine da

Scegliere il tipo di condizione da aggiungere alla regola:

- Condizioni di corrispondenza dello scripting tra siti: scegli abbina almeno uno dei filtri nella condizione di corrispondenza dello scripting tra siti
- Condizioni di corrispondenza IP: scegli l'origine da un indirizzo IP in
- Condizioni di corrispondenza geografica: scegli la provenienza da una posizione geografica in
- Condizioni di vincolo di dimensione: scegli abbina almeno uno dei filtri nella condizione di vincolo di dimensione
- Condizioni di corrispondenza di iniezione SQL: scegli abbina almeno uno dei filtri nella condizione SQL injection match
- Condizioni di corrispondenza delle stringhe: scegli abbina almeno uno dei filtri nella condizione di corrispondenza delle stringhe
- Condizioni di corrispondenza regex: scegli abbina almeno uno dei filtri nella condizione di corrispondenza regex

nome della condizione

Scegliere la condizione da aggiungere alla regola. L'elenco visualizza solo le condizioni del tipo scelto nell'elenco precedente.

d. Per aggiungere un'altra condizione alla regola, scegliere Add another condition (Aggiungi un'altra condizione) e ripetere le fasi b e c. Tieni presente quanto segue:

- Se aggiungi più di una condizione, una richiesta web deve soddisfare almeno un filtro in ogni condizione affinché AWS WAF Classic consenta o blocchi le richieste basate su quella regola.
- Se aggiungi due condizioni di corrispondenza IP alla stessa regola, AWS WAF Classic consentirà o bloccherà solo le richieste che provengono da indirizzi IP che compaiono in entrambe le condizioni di corrispondenza IP.

e. Ripetere la fase 9 fino a quando non sono state create tutte le regole da aggiungere a questa ACL Web.

f. Scegli Crea.

g. Continuare con la fase 10.

10. Per ogni regola o gruppo di regole nell'ACL Web, scegli il tipo di gestione che desideri venga fornito da AWS WAF Classic, come segue:

- Per ogni regola, scegli se desideri che AWS WAF Classic consenta, blocchi o conteggi le richieste Web in base alle condizioni della regola:
  - Consenti: API Gateway CloudFront o Application Load Balancer risponde con l'oggetto richiesto. Nel caso di CloudFront, se l'oggetto non si trova nella cache edge, CloudFront inoltra la richiesta all'origine.
  - Block: API Gateway CloudFront o Application Load Balancer risponde alla richiesta con un codice di stato HTTP 403 (Forbidden). CloudFront può anche rispondere con una pagina di errore personalizzata. Per ulteriori informazioni, consulta Utilizzo di AWS WAF Classic con pagine di errore CloudFront personalizzate.
  - Count: AWS WAF Classic incrementa un contatore di richieste che soddisfano le condizioni della regola, quindi continua a esaminare la richiesta Web in base alle regole rimanenti nell'ACL Web.

    Per ulteriori informazioni sull'utilizzo di Count (Conta) per testare un'ACL Web prima di iniziare a utilizzarla per consentire o bloccare le richieste Web, consulta Conteggio delle richieste Web che corrispondono alle regole in un'ACL Web.
- Per ogni gruppo di regole, impostare l'operazione di sostituzione per il gruppo di regole:
  - Nessuna sovrascrittura: consente l'utilizzo delle azioni delle singole regole all'interno del gruppo di regole.
  - Sostituisci per contare: sostituisce tutte le azioni di blocco specificate dalle singole regole del gruppo, in modo che vengano conteggiate solo tutte le richieste corrispondenti.

Per ulteriori informazioni, consulta Sostituzione del gruppo di regole.

11. Se desideri modificare l'ordine delle regole nell'ACL web, usa le frecce nella colonna Ordine. AWS WAF Classic esamina le richieste Web in base all'ordine in cui le regole vengono visualizzate nell'ACL Web.
12. Se si desidera rimuovere una regola aggiunta all'ACL Web, scegliere la x nella riga per la regola.
13. Scegliere l'operazione predefinita per l'ACL Web. Questa è l'azione che AWS WAF Classic esegue quando una richiesta web non soddisfa le condizioni di nessuna delle regole di questo ACL web. Per ulteriori informazioni, consulta Decisione dell'operazione predefinita per un'ACL Web.
14. Scegliere Review and create (Rivedi e crea).
15. Esaminare le impostazioni per l'ACL Web e scegliere Confirm and create (Conferma e crea).

Associazione o dissociazione di un ACL Web con un'API Amazon API Gateway, una CloudFront distribuzione o un Application Load Balancer

> **Note**
>
> Questa è la documentazione classica.AWS WAF Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Per associare o dissociare un'ACL Web, eseguire la procedura applicabile. Tieni presente che puoi anche associare un ACL Web a una CloudFront distribuzione quando crei o aggiorni la distribuzione. Per ulteriori informazioni, consulta Using AWS WAF Classic per controllare l'accesso ai tuoi contenuti nella Amazon CloudFront Developer Guide.

Le seguenti limitazioni si applicano durante l'associazione di un'ACL Web:

- Ogni API API Gateway, Application Load Balancer e CloudFront distribuzione possono essere associati a un solo ACL web.

- Gli ACL Web associati a una CloudFront distribuzione non possono essere associati a un'API Application Load Balancer o API Gateway. L'ACL web può, tuttavia, essere associato ad altre distribuzioni. CloudFront

Per associare un ACL Web a un'API Gateway API, una CloudFront distribuzione o un Application Load Balancer

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).
3. Scegli il nome dell'ACL web che desideri associare a un'API API Gateway API, a una CloudFront distribuzione o a un Application Load Balancer. Si apre una pagina con i dettagli dell'ACL Web nel riquadro a destra.
4. Nella scheda Regole, in AWS Risorse che utilizzano questo ACL web, scegli Aggiungi associazione.
5. Quando richiesto, utilizzate l'elenco delle risorse per scegliere l'API API Gateway, la CloudFront distribuzione o l'Application Load Balancer a cui desiderate associare questo ACL web. Se si sceglie un Application Load Balancer, è necessario specificare anche una regione.
6. Scegli Aggiungi.
7. Per associare questo ACL Web a un'API Gateway API aggiuntiva, a una CloudFront distribuzione o a un altro Application Load Balancer, ripeti i passaggi da 4 a 6.

Per dissociare un ACL Web da un'API Gateway API, una CloudFront distribuzione o un Application Load Balancer

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).
3. Scegli il nome dell'ACL web che desideri dissociare da un'API API Gateway, una CloudFront distribuzione o un Application Load Balancer. Si apre una pagina con i dettagli dell'ACL Web nel riquadro a destra.

4. Nella scheda Regole, in AWS Risorse che utilizzano questo ACL Web, scegli la x per ogni API API Gateway, CloudFront distribuzione o Application Load Balancer da cui desideri dissociare questo ACL Web.

Modifica di un'ACL Web

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Per aggiungere o rimuovere regole da un'ACL Web o modificare l'operazione predefinita, eseguire la procedura seguente.

Per modificare un'ACL Web

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).
3. Scegliere l'ACL Web che si desidera modificare. Si apre una pagina con i dettagli dell'ACL Web nel riquadro a destra.
4. Nella scheda Rules (Regole) nel riquadro a destra, scegliere Edit web ACL (Modifica ACL Web).
5. Per aggiungere regole all'ACL Web, procedere nel seguente modo:
   a. Nell'elenco Rules (Regole), scegliere la regola da aggiungere.
   b. Scegliere Add rule to web ACL (Aggiungi regola all'ACL Web).
   c. Ripetere le fasi a e b fino a quando non sono state aggiunte tutte le regole desiderate.
6. Se desideri modificare l'ordine delle regole nell'ACL web, usa le frecce nella colonna Ordine. AWS WAF Classic esamina le richieste Web in base all'ordine in cui le regole vengono visualizzate nell'ACL Web.

7. Per rimuovere una regola dall'ACL Web, scegliere la x a destra della riga per tale regola. Questa operazione non elimina la regola dalla AWS WAF versione classica, ma semplicemente la rimuove da questo ACL web.
8. Per modificare l'operazione per una regola o l'operazione predefinita per l'ACL Web, scegliere l'opzione preferita.

   > **Note**
   >
   > Quando si imposta l'azione per un gruppo di regole o un gruppo di Marketplace AWS regole (al contrario di una singola regola), l'azione impostata per il gruppo di regole (Nessuna sostituzione o Sostituisci per contare) viene chiamata azione di sostituzione. Per ulteriori informazioni, consulta Sostituzione del gruppo di regole

9. Scegli Save changes (Salva modifiche).

Eliminazione di un'ACL Web

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Per eliminare un ACL Web, è necessario rimuovere le regole incluse nell'ACL Web e dissociare tutte le CloudFront distribuzioni e gli Application Load Balancer dall'ACL Web. Esegui la seguente procedura.

Per eliminare un'ACL Web

1. Accedere e aprire la console all'indirizzo https://console.aws.amazon.com/wafv2/. AWS Management ConsoleAWS WAF

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.

2. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).

3. Scegli il nome dell'ACL web che desideri eliminare. Si apre una pagina con i dettagli dell'ACL Web nel riquadro a destra.
4. Nella scheda Rules (Regole) nel riquadro a destra, scegliere Edit web ACL (Modifica ACL Web).
5. Per rimuovere tutte le regole dall'ACL Web, scegliere la x a destra della riga per ogni regola. Ciò non elimina le regole dalla AWS WAF versione classica, ma semplicemente le rimuove da questo ACL web.
6. Scegli Aggiorna.
7. Dissocia l'ACL Web da tutte le CloudFront distribuzioni e dagli Application Load Balancer. Nella scheda Regole, in AWS Risorse che utilizzano questo ACL Web, scegli la x per ogni API API Gateway API, CloudFront distribuzione o Application Load Balancer.
8. Nella pagina Web ACLs (ACL Web), verificare che sia selezionata l'ACL Web da eliminare, quindi scegliere Delete (Elimina).

Test delle ACL Web

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Per evitare di configurare accidentalmente AWS WAF Classic per bloccare le richieste Web che desideri consentire o consentire le richieste che desideri bloccare, ti consigliamo di testare accuratamente l'ACL Web prima di iniziare a utilizzarlo sul tuo sito Web o sull'applicazione Web.

Argomenti

- Conteggio delle richieste Web che corrispondono alle regole in un'ACL Web
- Visualizzazione di un esempio di richieste Web che API Gateway CloudFront o un Application Load Balancer hanno inoltrato a Classic AWS WAF

Conteggio delle richieste Web che corrispondono alle regole in un'ACL Web

Quando aggiungi regole a un ACL Web, specifichi se desideri che AWS WAF Classic consenta, blocchi o conteggi le richieste Web che soddisfano tutte le condizioni di quella regola. Consigliamo di iniziare con la seguente configurazione:

- Configura tutte le regole di un'ACL Web per contare le richieste Web
- Imposta l'operazione predefinita per l'ACL Web per consentire le richieste

In questa configurazione, AWS WAF Classic esamina ogni richiesta Web in base alle condizioni della prima regola. Se la richiesta Web soddisfa tutte le condizioni di quella regola, AWS WAF Classic incrementa un contatore per quella regola. Quindi AWS WAF Classic esamina la richiesta web in base alle condizioni della regola successiva. Se la richiesta soddisfa tutte le condizioni di quella regola, AWS WAF Classic incrementa un contatore per la regola. Questo continua fino a quando AWS WAF Classic non ha esaminato la richiesta in base alle condizioni di tutte le tue regole.

Dopo aver configurato tutte le regole in un ACL Web per contare le richieste e aver associato l'ACL Web a un'API Amazon API Gateway, una CloudFront distribuzione o un Application Load Balancer, puoi visualizzare i conteggi risultanti in un grafico Amazon. CloudWatch Per ogni regola in un ACL Web e per tutte le richieste che API Gateway CloudFront o Application Load Balancer inoltra AWS WAF a Classic for a Web CloudWatch ACL, consente di:

- Visualizzare i dati per l'ora precedente o le tre ore precedenti
- Modificare l'intervallo tra punti dati
- Modifica il calcolo che viene CloudWatch eseguito sui dati, ad esempio massimo, minimo, media o somma

> **Note**
>
> AWS WAF Classic with CloudFront è un servizio globale e le metriche sono disponibili solo quando scegli la regione Stati Uniti orientali (Virginia settentrionale) nella. AWS Management Console Se scegli un'altra regione, nella console non verrà visualizzata alcuna metrica AWS WAF classica. CloudWatch

Per visualizzare i dati per le regole di un'ACL Web

1. Accedi AWS Management Console e apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, in Metrics (Parametri), scegliere WAF.
3. Selezionare la casella di controllo per l'ACL Web da aggiornare.
4. Modificare le impostazioni applicabili:

   Statistic

   Scegli il calcolo da CloudWatch eseguire sui dati.

   Intervallo temporale

   Scegliere se visualizzare i dati per l'ora precedente o le tre ore precedenti.

   Periodo

   Scegliere l'intervallo tra punti dati nel grafico.

   Regolamento

   Scegliere le regole per cui visualizzare i dati.

   Tieni presente quanto segue:

   - Se hai appena associato un ACL Web a un'API Gateway API, una CloudFront distribuzione o un Application Load Balancer, potresti dover attendere alcuni minuti prima che i dati vengano visualizzati nel grafico e che la metrica per l'ACL Web compaia nell'elenco delle metriche disponibili.
   - Se associ più di un'API API Gateway, una CloudFront distribuzione o un Application Load Balancer a un ACL web, i CloudWatch dati includeranno tutte le richieste per tutte le distribuzioni associate all'ACL web.
   - È possibile passare il cursore su un punto dati per ottenere ulteriori informazioni.
   - Il grafico non si aggiorna automaticamente. Per aggiornare la visualizzazione, scegliere l'icona di aggiornamento
     ().
5. (Facoltativo) Visualizza informazioni dettagliate sulle singole richieste che API Gateway CloudFront o un Application Load Balancer hanno inoltrato a Classic. AWS WAF Per ulteriori

informazioni, consulta Visualizzazione di un esempio di richieste Web che API Gateway CloudFront o un Application Load Balancer hanno inoltrato a Classic AWS WAF.

6. Se si determina che una regola intercetta le richieste che non si desidera vengano intercettate, modificare le impostazioni applicabili. Per ulteriori informazioni, consulta Creazione e configurazione di una lista di controllo accessi Web (ACL).

   Dopo aver verificato che tutte le regole intercettano solo le richieste corrette, modificare l'operazione per ciascuna delle regole su Allow (Consenti) o Block (Blocca). Per ulteriori informazioni, consulta Modifica di un'ACL Web.

Visualizzazione di un esempio di richieste Web che API Gateway CloudFront o un Application Load Balancer hanno inoltrato a Classic AWS WAF

Nella console AWS WAF Classic, puoi visualizzare un esempio delle richieste che API Gateway CloudFront o un Application Load Balancer hanno inoltrato a AWS WAF Classic per l'ispezione. Per ogni richiesta campionata, è possibile visualizzare i dati dettagliati sulla richiesta, ad esempio l'indirizzo IP di origine e le intestazioni incluse nella richiesta. È anche possibile visualizzare la regola corrispondente alla richiesta e se la regola viene configurata in modo da consentire o bloccare le richieste.

Il campione di richieste contiene fino a un massimo di 100 richieste corrispondenti a tutte le condizioni in ogni regola e altre 100 richieste per l'operazione predefinita, che si applica alle richieste che non corrispondono a tutte le condizioni in ogni regola. Le richieste nell'esempio provengono da tutte le API API Gateway, dalle CloudFront edge location o dagli Application Load Balancer che hanno ricevuto richieste per i tuoi contenuti nei 15 minuti precedenti.

Per visualizzare un esempio delle richieste Web che API Gateway CloudFront o un Application Load Balancer hanno inoltrato a Classic AWS WAF

1. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.

2. Nel riquadro di navigazione, scegliere l'ACL Web per cui visualizzare le richieste.
3. Nel riquadro a destra, selezionare la scheda Requests (Richieste).

   Nella tabella Sampled requests (Richieste campionate) vengono visualizzati i seguenti valori per ogni richiesta:

IP di origine

L'indirizzo IP da cui proviene la richiesta oppure, se il visualizzatore ha utilizzato un proxy HTTP o un Application Load Balancer per inviare la richiesta, l'indirizzo IP del proxy o dell'Application Load Balancer.

URI

Il percorso URI della richiesta, che identifica la risorsa, ad esempio,. `/images/daily-ad.jpg` Ciò non include la stringa di query o i componenti del frammento dell'URI. Per informazioni, vedete Uniform Resource Identifier (URI): sintassi generica.

Regola di corrispondenza

Identifica la prima regola dell'ACL Web per cui la richiesta Web corrispondeva a tutte le condizioni. Se una richiesta Web non soddisfa tutte le condizioni di nessuna regola nell'ACL Web, il valore della regola Matches è Default.

Tieni presente che quando una richiesta Web soddisfa tutte le condizioni di una regola e l'azione per quella regola è Count, AWS WAF Classic continua a esaminare la richiesta Web in base alle regole successive nell'ACL Web. In questo caso, una richiesta Web può venire visualizzata due volte nell'elenco di richieste campionate: una volta per la regola che ha un'operazione Count (Conta) e nuovamente per una regola successiva o per l'operazione predefinita.

Azione

Indica se l'operazione per la regola corrispondente è Allow (Consenti), Block (Blocca) o Count (Conta).

Orario

L'ora in cui AWS WAF Classic ha ricevuto la richiesta da API Gateway CloudFront o dal tuo Application Load Balancer.

4. Per visualizzare informazioni aggiuntive sulla richiesta, scegli la freccia sul lato sinistro dell'indirizzo IP della richiesta. AWS WAF Classic visualizza le seguenti informazioni:

IP di origine

Lo stesso indirizzo IP del valore nella colonna Source IP (IP di origine) nella tabella.

Paese

Il codice paese a due lettere del paese da cui la richiesta ha avuto origine. Se il visualizzatore ha utilizzato un proxy HTTP o un Application Load Balancer per inviare la richiesta, questo è il codice del paese a due lettere del paese in cui si trova il proxy HTTP o un Application Load Balancer.

Per un elenco di codici paese a due lettere e i nomi dei paesi corrispondenti, consulta la voce Wikipedia ISO 3166-1 alpha-2.

Metodo

Il metodo della richiesta HTTP per la richiesta: `GET`, `HEAD`, `OPTIONS`, `PUT`, `POST`, `PATCH` o `DELETE`.

URI

Lo stesso URI del valore nella colonna URI nella tabella.

Intestazioni della richiesta

Le intestazioni della richiesta e i valori dell'intestazione nella richiesta.

5. Per aggiornare l'elenco delle richieste di esempio, scegliere Get new samples (Ottieni nuovi campioni).

Utilizzo dei gruppi di regole AWS WAF classici da utilizzare con AWS Firewall Manager

> **Note**
>
> Questa è la documentazione di AWS WAF Classic. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Un gruppo di regole AWS WAF classico è un insieme di regole che si aggiungono a una AWS Firewall Manager politica AWS WAF classica. È possibile creare il proprio gruppo di regole oppure acquistare un gruppo di regole gestito da Marketplace AWS.

> **Important**
>
> Se desideri aggiungere un gruppo di Marketplace AWS regole alla tua politica di Firewall Manager, ogni account dell'organizzazione deve prima iscriversi a quel gruppo di regole. Una volta effettuata la sottoscrizione di tutti gli account, è possibile aggiungere il gruppo di regole a una policy. Per ulteriori informazioni, consulta Marketplace AWS gruppi di regole.

Argomenti

Creazione di un gruppo di regole AWS WAF classico

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Quando si crea un gruppo di regole AWS WAF classico da utilizzare con AWS Firewall Manager, si specifica quali regole aggiungere al gruppo.

Per creare un gruppo di regole (console)

1. Accedere AWS Management Console utilizzando l'account AWS Firewall Manager amministratore impostato nei prerequisiti, quindi aprire la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fms.

> **Note**
>
> Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare Passaggio 2: creare un account amministratore AWS Firewall Manager predefinito.

2. Nel pannello di navigazione, scegli Passa alla AWS WAF versione classica.
3. Nel riquadro di navigazione AWS WAF classico, scegli Gruppi di regole.
4. Scegliere Create rule group (Crea gruppo di regole).

> **Note**
>
> Non è possibile aggiungere regole basate sulla frequenza a un gruppo di regole.

5. Se le regole che si desidera aggiungere al gruppo di regole sono già state create, scegliere Use existing rules for this rule group (Usa regole esistenti per questo gruppo di regole). Se si desidera creare nuove regole da aggiungere al gruppo di regole, scegliere Create rules and conditions for this rule group (Crea regole e condizioni per questo gruppo di regole).
6. Seleziona Successivo.
7. Se si sceglie di creare regole, seguire le fasi per crearle in Creazione di una regola e aggiunta di condizioni.

> **Note**
>
> Usa la console AWS WAF Classic per creare le tue regole.

   Dopo aver creato tutte le regole necessarie, passare alla fase successiva.
8. Digitare un nome per il gruppo di regole.
9. Per aggiungere una regola al gruppo di regole, selezionare una regola, quindi scegliere Add rule (Aggiungi regola). Scegliere se consentire, bloccare o contare le richieste che soddisfano le condizioni della regola. Per ulteriori informazioni sulle scelte, consulta Come funziona AWS WAF Classic.
10. Al termine dell'aggiunta delle regole, scegliere Create (Crea).

È possibile testare il gruppo di regole aggiungendolo a un AWS WAF WebACL e impostando l'azione WebACL su Override to Count. Questa operazione sostituisce qualsiasi operazione scelta per le regole contenute nel gruppo e conta solo le richieste corrispondenti. Per ulteriori informazioni, consulta Creazione di un'ACL Web.

Aggiungere ed eliminare regole da un gruppo di regole AWS WAF classico

> **Note**
>
> Questa è la documentazione della AWS WAF versione classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF. Per la versione più recente di AWS WAF, vedi. AWS WAF

È possibile aggiungere o eliminare regole in un gruppo di regole AWS WAF classico.

L'eliminazione di una regola dal gruppo di regole non elimina la regola stessa. L'operazione rimuove la regola solo dal gruppo di regole.

Per aggiungere o eliminare regole in un gruppo di regole (console)

1. Accedere AWS Management Console utilizzando l'account AWS Firewall Manager amministratore impostato nei prerequisiti, quindi aprire la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fms.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare Passaggio 2: creare un account amministratore AWS Firewall Manager predefinito.

2. Nel pannello di navigazione, scegli Passa alla AWS WAF versione classica.
3. Nel riquadro di navigazione AWS WAF classico, scegli Gruppi di regole.
4. Scegliere il gruppo di regole da eliminare.
5. Scegliere Edit rule group (Modifica gruppo di regole).
6. Per aggiungere regole, procedere nel seguente modo:

a. Selezionare una regola, quindi scegliere Add rule to rule group (Aggiungi regola al gruppo di regole). Scegliere se consentire, bloccare o contare le richieste che soddisfano le condizioni della regola. Per ulteriori informazioni sulle scelte, consulta Come funziona AWS WAF Classic. Ripetere per aggiungere altre regole al gruppo di regole.

> **Note**
>
> Non è possibile aggiungere regole basate sulla frequenza al gruppo di regole.

b. Scegli Aggiorna.

7. Per eliminare regole, procedere nel seguente modo:

a. Scegliere la X accanto alla regola da eliminare. Ripetere per eliminare altre regole dal gruppo di regole.

b. Scegli Aggiorna.

Guida introduttiva AWS Firewall Manager all'attivazione delle regole AWS WAF classiche

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Puoi utilizzarlo AWS Firewall Manager per abilitare AWS WAF regole, regole AWS WAF classiche, AWS Shield Advanced protezioni e gruppi di sicurezza Amazon VPC. I passaggi per la configurazione sono leggermente diversi per ciascuno.

- Per utilizzare Firewall Manager per abilitare le regole utilizzando la versione più recente di AWS WAF, non utilizzare questo argomento. Seguire invece la seguente procedura riportata in Guida introduttiva alle AWS Firewall ManagerAWS WAF politiche.

- Per utilizzare Firewall Manager per abilitare AWS Shield Advanced le protezioni, procedi nel Guida introduttiva alle AWS Firewall ManagerAWS Shield Advanced politiche seguente modo.
- Per utilizzare Firewall Manager per abilitare i gruppi di sicurezza Amazon VPC, segui la procedura riportata di seguito. Guida introduttiva alle policy dei gruppi di sicurezza di AWS Firewall Manager Amazon VPC

Per utilizzare Firewall Manager per abilitare le regole AWS WAF classiche, eseguire i seguenti passaggi in sequenza.

Argomenti

Fase 1: completamento dei prerequisiti

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Vi sono diversi passaggi obbligatori per preparare l'account AWS Firewall Manager. Tali fasi sono descritte nell'articolo AWS Firewall Manager prerequisiti. Completare tutti i prerequisiti prima di passare a Fase 2: creazione delle regole.

Fase 2: creazione delle regole

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e

non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
Per la versione più recente di AWS WAF, vedi. AWS WAF

In questo passaggio, crei regole utilizzando AWS WAF Classic. Se hai già delle regole AWS WAF classiche che desideri utilizzare AWS Firewall Manager, salta questo passaggio e vai aFase 3: creazione di un gruppo di regole.

> **Note**
>
> Usa la console AWS WAF Classic per creare le tue regole.

Per creare regole AWS WAF classiche (console)

- Creare le regole, quindi aggiungere le proprie condizioni alle regole. Per ulteriori informazioni, consulta Creazione di una regola e aggiunta di condizioni.

È possibile ora procedere a Fase 3: creazione di un gruppo di regole.

Fase 3: creazione di un gruppo di regole

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Un gruppo di regole è un set di regole che definisce quali operazioni intraprendere quando viene soddisfatto un determinato set di condizioni. È possibile utilizzare gruppi di regole gestiti da Marketplace AWS e creare gruppi di regole personalizzati. Per informazioni sui gruppi di regole gestite, consulta Marketplace AWS gruppi di regole.

Per creare il proprio gruppo di regole, eseguire la procedura seguente.

Per creare un gruppo di regole (console)

1. Accedere AWS Management Console utilizzando l'account AWS Firewall Manager amministratore impostato nei prerequisiti, quindi aprire la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fms.
2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Se i prerequisiti non sono stati soddisfatti, la console visualizzerà le istruzioni su come risolvere eventuali problemi. Seguire le istruzioni, quindi iniziare di nuovo questa fase (creazione di un gruppo di regole). Se i requisiti sono stati soddisfatti, scegliere Close (Chiudi).
4. Scegli Crea policy.

   Per Policy type (Tipo di policy), scegliere AWS WAF Classic.
5. Scegli Crea una AWS Firewall Manager politica e aggiungi un nuovo gruppo di regole.
6. Scegli un Regione AWS, quindi scegli Avanti.
7. Avendo già creato regole, non è necessario creare le condizioni. Seleziona Successivo.
8. Avendo già creato regole, non è necessario creare le regole. Seleziona Successivo.
9. Scegliere Create rule group (Crea gruppo di regole).
10. Per Name (Nome), inserire un nome descrittivo.
11. Inserisci un nome per la CloudWatch metrica che AWS WAF Classic creerà e assocerà al gruppo di regole. Il nome può contenere solo caratteri alfanumerici (A - Z, a - z, 0 - 9) o i seguenti caratteri speciali: _-!"#`+*},./. Non può contenere spazi.
12. Selezionare una regola, quindi scegliere Add rule (Aggiungi regola). Una regola ha un'impostazione di operazione che consente di scegliere se consentire, bloccare o contare le richieste che soddisfano le condizioni della regola. Per questo tutorial, scegliere Count (Contare). Ripetere l'aggiunta di regole finché tutte le regole non vengono aggiunte al gruppo di regole.
13. Scegli Crea.

È possibile ora procedere a Fase 4: Creare e applicare un criterio AWS Firewall ManagerAWS WAF classico.

Fase 4: Creare e applicare un criterio AWS Firewall ManagerAWS WAF classico

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Dopo aver creato il gruppo di regole, si crea una AWS Firewall Manager AWS WAF policy. Una AWS WAF policy di Firewall Manager contiene il gruppo di regole da applicare alle risorse.

Per creare una AWS WAF policy di Firewall Manager (console)

1. Dopo aver creato il gruppo di regole (l'ultima fase della procedura precedente, Fase 3: creazione di un gruppo di regole), la console mostrerà la pagina Rule group summary (Riepilogo del gruppo di regole). Seleziona Successivo.
2. Per Name (Nome), inserire un nome descrittivo.
3. Per Policy type (Tipo di policy), scegliere WAF.
4. Per Regione, scegli un Regione AWS. Per proteggere CloudFront le risorse di Amazon, scegli Global.

   Per proteggere le risorse in più aree (diverse dalle CloudFront risorse), è necessario creare policy Firewall Manager separate per ogni regione.
5. Selezionare un gruppo di regole da aggiungere, quindi scegliere Add rule group (Aggiungi gruppo di regole).
6. È possibile eseguire due operazioni su una policy: Action set by rule group (Operazione impostata dal gruppo di regole) e Count (Contare). Se si desidera verificare la policy e il gruppo di regole, impostare l'operazione su Count (Contare). Questa operazione sostituisce tutte le operazioni di blocco specificate dal gruppo di regole contenute nella policy. In altre parole, se l'operazione della policy è impostata su Count (Contare), le relative richieste vengono solo contate, non bloccate. Al contrario, se l'operazione della policy è impostata su Action set by rule

group (Operazione impostata dal gruppo di regole), vengono utilizzate le operazioni del gruppo di regole nella policy. Per questo tutorial, scegliere Count (Contare).

7. Seleziona Successivo.
8. Se si desidera includere solo gli account specifici nelle policy o in alternativa escludere gli account specifici dalla policy, selezionare Select accounts to include/exclude from this policy (optional) (seleziona gli account da includere o escludere da questa policy, facoltativo). Scegliere se Include only these accounts in this policy (Includere solo questi account nella policy) o Exclude these accounts from this policy (Escludere questi account dalla policy). È possibile scegliere una sola opzione. Scegli Aggiungi. Selezionare il numero di account da includere o escludere quindi scegliere OK.

   > **Note**
   >
   > Se non si seleziona questa opzione, Firewall Manager applica una politica a tutti gli account dell'organizzazione in AWS Organizations. Se si aggiunge un nuovo account all'organizzazione, Firewall Manager applica automaticamente la politica a quell'account.

9. Scegliere i tipi di risorse da proteggere.
10. Se si desidera proteggere solo le risorse con tag specifici oppure escludere le risorse con tag specifici, selezionare Use tags to include/exclude resources (Usa tag per includere/escludere risorse), inserire i tag e quindi scegliere Include (Includi) o Exclude (Escludi). È possibile scegliere una sola opzione.

    Se inserisci più di un tag (separati da virgole) e se una risorsa presenta uno di questi tag, viene considerata una corrispondenza.

    Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .
11. Scegliere Create and apply this policy to existing and new resources (Crea e applica questa policy alle risorse esistenti e alle nuove risorse).

    Questa opzione crea un ACL Web in ogni account applicabile all'interno di un'organizzazione in AWS Organizations e lo associa alle risorse specificate negli account. Inoltre, questa opzione applica la policy a tutte le nuove risorse che soddisfano i criteri precedenti (tipo di risorsa e tag). In alternativa, se si sceglie Crea ma non si applica questo criterio a risorse esistenti o nuove, Firewall Manager crea un ACL Web in ogni account applicabile all'interno dell'organizzazione, ma non lo applica a nessuna risorsa. In seguito sarà necessario applicare la policy alle risorse.

12. Lasciare la scelta per Replace existing associated web ACLs (Sostituire gli ACL Web associati esistenti) all'impostazione predefinita.

    Quando questa opzione è selezionata, Firewall Manager ha rimosso tutte le associazioni ACL Web esistenti dalle risorse dell'ambito prima di associare ad esse gli ACL Web della nuova policy.
13. Seleziona Successivo.
14. Rivedere la nuova policy. Per apportare una modifica, scegliere Edit (Modifica). Al termine, scegliere Create policy (Crea policy).

Tutorial: creazione di una policy AWS Firewall Manager con regole gerarchiche

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Con AWS Firewall Manager, è possibile creare e applicare politiche di protezione AWS WAF classiche che contengono regole gerarchiche. In altre parole, è possibile creare e applicare determinate regole in modo centralizzato, ma delegare la creazione e la gestione di regole specifiche per account ad altri individui. È possibile monitorare le regole (comuni) applicate in modo centralizzato per rilevare eventuali rimozioni o manomissioni accidentali in modo da accertarsi che vengano applicate costantemente. Le regole specifiche per account aggiungono un'ulteriore protezione personalizzata per le esigenze dei singoli team.

> **Note**
>
> Nell'ultima versione di AWS WAF, questa funzionalità è integrata e non richiede alcuna gestione speciale. Se non stai già utilizzando AWS WAF Classic, utilizza invece la versione

più recente. Per informazioni, consulta Creazione di una AWS Firewall Manager politica per AWS WAF.

Il seguente tutorial descrive come creare un set di regole di protezione gerarchiche.

Argomenti

Fase 1: Designare un account amministratore di Firewall Manager

Per utilizzarlo AWS Firewall Manager, è necessario designare un account dell'organizzazione come account amministratore di Firewall Manager. Questo account può essere l'account di gestione o un account membro dell'organizzazione.

È possibile utilizzare l'account amministratore di Firewall Manager per creare un set di regole comuni da applicare ad altri account dell'organizzazione. Gli altri account dell'organizzazione non possono modificare queste regole applicate in modo centralizzato.

Per designare un account come account amministratore di Firewall Manager e completare altri prerequisiti per l'utilizzo di Firewall Manager, vedere le istruzioni riportate in. AWS Firewall Manager prerequisiti Se i prerequisiti sono già stati completati, è possibile passare alla fase 2 di questo tutorial.

In questo tutorial ci si riferisce all'account amministratore come **`Firewall-Administrator-Account`**.

Passaggio 2: creare un gruppo di regole utilizzando l'account amministratore di Firewall Manager

Quindi, creare un gruppo di regole utilizzando **`Firewall-Administrator-Account`**. Questo gruppo di regole contiene le regole comuni che si applicano a tutti gli account membri gestiti dalla policy creata nella fase successiva. Solo **`Firewall-Administrator-Account`** può modificare queste regole e il gruppo di regole contenitore.

In questo tutorial, ci si riferisce a questo gruppo di regole contenitore come **`Common-Rule-Group`**.

Per creare un gruppo di regole, consultare le istruzioni in Creazione di un gruppo di regole AWS WAF classico. Ricordarsi di accedere alla console utilizzando l'account amministratore di Firewall Manager (**`Firewall-Administrator-Account`**) quando si seguono queste istruzioni.

Fase 3: Creare una policy di Firewall Manager e allegare il gruppo di regole comune

Utilizzando**`Firewall-Administrator-Account`**, crea una policy Firewall Manager. Quando si crea questa policy, è necessario procedere come segue:

- Aggiungere **`Common-Rule-Group`** alla nuova policy.
- Includere tutti gli account dell'organizzazione a cui si desidera applicare **`Common-Rule-Group`**.
- Aggiungere tutte le risorse a cui si desidera applicare **`Common-Rule-Group`**.

Per istruzioni sulla creazione di una policy, consultare Creazione di una AWS Firewall Manager politica.

Questo crea un'ACL Web in ogni account specificato e aggiunge **`Common-Rule-Group`** a ognuna di queste ACL Web. Una volta creata la policy, questa ACL Web e le regole comuni vengono distribuite a tutti gli account specificati.

In questo tutorial, ci si riferisce a questa ACL Web come **`Administrator-Created-ACL`**. A questo punto esiste un'**`Administrator-Created-ACL`** univoca in ogni account membro specificato dell'organizzazione.

Fase 4: aggiunta di regole specifiche per account

Ogni account membro dell'organizzazione ora può aggiungere le proprie regole specifiche per account all'**`Administrator-Created-ACL`** che esiste nel loro account. Le regole comuni già in vigore **`Administrator-Created-ACL`** continuano ad applicarsi, insieme alle nuove regole specifiche per gli account. AWS WAF esamina le richieste Web in base all'ordine in cui le regole vengono visualizzate nell'ACL Web. Ciò vale sia per l'**`Administrator-Created-ACL`** che per le regole specifiche per account.

Per aggiungere regole**`Administrator-Created-ACL`**, vedi. Modifica di un ACL Web

Conclusioni

Ora è disponibile un ACL Web che contiene regole comuni amministrate dall'account amministratore di Firewall Manager e regole specifiche dell'account gestite da ciascun account membro.

L'**`Administrator-Created-ACL`** in ogni account fa riferimento al singolo **`Common-Rule-Group`**. Pertanto, le future modifiche apportate dall'account amministratore di Firewall Manager **`Common-Rule-Group`** avranno effetto immediato in ogni account membro.

Gli account membri non possono modificare o eliminare le regole comuni in **`Common-Rule-Group`**.

Le regole specifiche per account non influiscono su altri account.

Registrazione informazioni di traffico ACL Web

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

È possibile attivare la registrazione per ottenere informazioni dettagliate sul traffico analizzato dall'ACL Web. Le informazioni contenute nei log includono l'ora in cui AWS WAF Classic ha ricevuto la richiesta dalla AWS risorsa, informazioni dettagliate sulla richiesta e l'azione relativa alla regola a cui ogni richiesta corrisponde.

Per iniziare, configurare un Amazon Kinesis Data Firehose. Come parte del processo, scegliere una destinazione per l'archiviazione dei log. Successivamente, scegli l'ACL Web per cui si desidera attivare la registrazione. Dopo aver abilitato la registrazione, AWS WAF invia i log alla destinazione di archiviazione tramite il firehose.

Per informazioni su come creare un Amazon Kinesis Data Firehose e rivedere i log memorizzati, consulta What Is Amazon Data Firehose? Per comprendere le autorizzazioni richieste per la configurazione di Kinesis Data Firehose, consulta Controlling Access with Amazon Kinesis Data Firehose.

È necessario disporre delle autorizzazioni seguenti per attivare la registrazione:

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `waf:PutLoggingConfiguration`

Per ulteriori informazioni sui ruoli collegati ai servizi e sull'autorizzazione `iam:CreateServiceLinkedRole`, consulta Utilizzo di ruoli collegati ai servizi per Classic AWS WAF.

Per attivare la registrazione per un ACL Web

1. Crea un Amazon Kinesis Data Firehose utilizzando un nome che inizia con il aws-waf-logs prefisso "-» Ad esempio,. `aws-waf-logs-us-east-2-analytics` Creare i dati firehose con un'origine PUT e nella regione in cui si sta lavorando. Se stai acquisendo log per Amazon CloudFront, crea la firehose negli Stati Uniti orientali (Virginia settentrionale). Per ulteriori informazioni, consulta Creating an Amazon Data Firehose Delivery Stream.

   > **Important**
   >
   > Non scegliere `Kinesis stream` come origine.
   > Un registro AWS WAF Classic equivale a un record Firehose. Se in genere ricevi 10.000 richieste al secondo e abiliti i log completi, dovresti avere un'impostazione di 10.000 record al secondo in Firehose. Se non configuri Firehose correttamente, AWS WAF Classic non registrerà tutti i log. Per ulteriori informazioni, consulta Quote di Amazon Kinesis Data Firehose.

2. Accedi AWS Management Console e apri la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
3. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).
4. Scegli il nome dell'ACL web per cui desideri abilitare la registrazione. Si apre una pagina con i dettagli dell'ACL Web nel riquadro a destra.
5. Nella scheda Logging (Registrazione), selezionare Enable logging (Attiva registrazione).
6. Scegliere la Kinesis Data Firehose creata durante la prima fase. Devi scegliere una manichetta antincendio che inizi con "aws-waf-logs-».

7. (Facoltativo) Se non si desidera che determinati campi e i relativi valori vengano inclusi nei log, omettere tali campi. Scegliere il campo da omettere, quindi selezionare Add (Aggiungi). Se necessario, ripetere l'operazione per omettere i campi aggiuntivi. I campi omessi vengono visualizzati come `REDACTED` nei log. Ad esempio, se si omette il campo cookie, il campo cookie nei log sarà `REDACTED`.
8. Scegliere Enable Logging (Attiva registrazione).

> **Note**
>
> Quando abiliti correttamente la registrazione, AWS WAF Classic creerà un ruolo collegato al servizio con le autorizzazioni necessarie per scrivere log su Amazon Kinesis Data Firehose. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Classic AWS WAF.

Per disabilitare la registrazione per un ACL Web

1. Nel riquadro di navigazione, scegliere Web ACLs (ACL Web).
2. Scegli il nome dell'ACL web per cui desideri disabilitare la registrazione. Si apre una pagina con i dettagli dell'ACL Web nel riquadro a destra.
3. Nella scheda Logging (Registrazione), selezionare Disable logging (Disabilita registrazione).
4. Nella finestra di dialogo, selezionare Disable logging (Disabilita registrazione).

Example Log di esempio


```
{

 "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"
                       }
}
```

Di seguito è riportata una spiegazione di ciascuna voce elencata in questi log:

timestamp

Time Stamp in millisecondi.

Tipo di formato

Tipo di formato per il log.

webaclId

GUID dell'ACL Web.

terminatingRuleId

ID della regola che ha terminato la richiesta. Se non viene terminata la richiesta, il valore è `Default_Action`.

terminatingRuleType

Tipo della regola che ha terminato la richiesta. Valori possibili: RATE_BASED, REGULAR e GROUP.

action

Operazione. Valori possibili per una regola di terminazione: ALLOW e BLOCK. COUNT non è un valore valido per una regola di terminazione.

terminatingRuleMatchDettagli

Informazioni dettagliate sulla regola di terminazione corrispondente alla richiesta. Una regola di terminazione ha un'azione che termina il processo di ispezione di una richiesta Web. Le possibili operazioni per una regola di terminazione sono ALLOW e BLOCK. Questo viene popolato solo per le istruzioni delle regole di corrispondenza SQL injection e Cross-site scripting (XSS). Come per tutte le istruzioni di regola che controllano più di un oggetto, AWS WAF applica l'operazione alla prima corrispondenza e interrompe l'ispezione della richiesta Web. Una richiesta Web con un'operazione di terminazione potrebbe contenere altre minacce, oltre a quella segnalata nel log.

httpSourceName

Origine della richiesta. Valori possibili: CF (se l'origine è Amazon CloudFront), APIGW (se l'origine è Amazon API Gateway) e ALB (se l'origine è un Application Load Balancer).

httpSourceId

ID origine. Questo campo mostra l'ID della CloudFront distribuzione Amazon associata, l'API REST per API Gateway o il nome di un Application Load Balancer.

ruleGroupList

Elenco dei gruppi di regole che hanno operato su questa richiesta. Nell'esempio di codice precedente, ce n'è uno solo.

ruleGroupId

ID del gruppo di regole. Se la regola ha bloccato la richiesta, l'ID per `ruleGroupID` è uguale all'ID per `terminatingRuleId`.

terminatingRule

Regola all'interno del gruppo di regole che hanno terminato la richiesta. Se questo è un valore non null, contiene anche ruleid e action. In questo caso, l'operazione sarà sempre BLOCK.

nonTerminatingMatchingRegole

L'elenco di regole nel gruppo di regole che corrispondono alla richiesta. Queste sono sempre regole di tipo COUNT (regole di non terminazione che corrispondono).

azione (gruppo nonTerminatingMatching Regole)

Questa è sempre una regola di tipo COUNT (regole di non terminazione che corrispondono).

RuleID (gruppo RulesnonTerminatingMatching)

ID della regola all'interno del gruppo di regole corrispondente alla richiesta e che non è di terminazione. Cioè regole COUNT.

excludedRules

L'elenco di regole nel gruppo di regole che sono state escluse. L'operazione impostata per queste regole è COUNT.

exclusionType (gruppo excludedRules)

Tipo che indica che la regola esclusa contiene l'operazione COUNT.

ruleId (gruppo excludedRules)

L'ID della regola all'interno del gruppo di regole che è esclusa.

rateBasedRuleElenco

Elenco dei gruppi di regole basate su tariffa che hanno operato su questa richiesta.

rateBasedRuleId

ID della regola basata sulla frequenza che ha operato su questa richiesta. Se ciò ha terminato la richiesta, l'ID di `rateBasedRuleId` è uguale all'ID di `terminatingRuleId`.

limitKey

Il campo AWS WAF utilizzato per determinare se è probabile che le richieste arrivino da un'unica fonte e quindi siano soggette al monitoraggio della frequenza. Valore possibile: IP.

maxRateAllowed

Numero massimo di richieste, che hanno lo stesso valore nel campo specificato da `limitKey`, consentite in un periodo di tempo di cinque minuti. Se il numero di richieste supera il `maxRateAllowed` e vengono soddisfatti anche gli altri predicati specificati nella regola, AWS WAF attiva l'azione specificata per questa regola.

httpRequest

Metadati sulla richiesta.

clientIp

Indirizzo IP del client che invia la richiesta.

country

Paese di origine della richiesta. Se non AWS WAF è in grado di determinare il paese di origine, imposta questo campo su. -

headers

Elenco intestazioni.

uri

URI della richiesta. Il precedente esempio di codice illustra quale sarebbe il valore se il campo venisse omesso.

args

Stringa query.

httpVersion

Versione HTTP.

httpMethod

Metodo HTTP nella richiesta.

requestId

ID della richiesta.

Elenco degli indirizzi IP bloccati dalle regole basate sulla frequenza

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

AWS WAF Classic fornisce un elenco di indirizzi IP bloccati da regole basate sulla velocità.

Per visualizzare gli indirizzi IP bloccati dalle regole basate sulla frequenza

1. Accedere AWS Management Console e aprire la AWS WAF console all'indirizzo https://console.aws.amazon.com/wafv2/.

   Se vedi Passa alla AWS WAF versione classica nel riquadro di navigazione, selezionalo.
2. Nel pannello di navigazione, scegli Regole.
3. Nella colonna Name (Nome), scegliere una regola basata sulla frequenza.

   L'elenco mostra gli indirizzi IP attualmente bloccati dalla regola.

Come funziona AWS WAF Classic con le CloudFront funzionalità di Amazon

> **Note**
>
> Questa è la documentazione di AWS WAF Classic. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Quando crei un ACL Web, puoi specificare una o più CloudFront distribuzioni che desideri che AWS WAF Classic analizzi. AWS WAF Classic inizia a consentire, bloccare o contare le richieste Web per tali distribuzioni in base alle condizioni identificate nell'ACL Web. CloudFront offre alcune funzionalità che migliorano la funzionalità AWS WAF Classic. Questo capitolo descrive alcuni modi in cui è possibile configurare CloudFront per far CloudFront funzionare meglio insieme AWS WAF Classic.

Argomenti

- Utilizzo di AWS WAF Classic con pagine di errore CloudFront personalizzate
- Utilizzo di AWS WAF Classic with CloudFront per le applicazioni in esecuzione sul tuo server HTTP
- Scelta dei metodi HTTP che CloudFront rispondono a

Utilizzo di AWS WAF Classic con pagine di errore CloudFront personalizzate

Quando AWS WAF Classic blocca una richiesta Web in base alle condizioni specificate, restituisce il codice di stato HTTP 403 (Forbidden) a CloudFront. Successivamente, CloudFront restituisce quel codice di stato al visualizzatore. Il visualizzatore quindi mostra un messaggio predefinito, breve e scarsamente formattato, simile a questo:

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

Se preferisci visualizzare un messaggio di errore personalizzato, possibilmente utilizzando la stessa formattazione del resto del sito Web, puoi configurare la restituzione CloudFront al visualizzatore di un oggetto (ad esempio un file HTML) che contenga il tuo messaggio di errore personalizzato.

> **Note**
>
> CloudFront non è in grado di distinguere tra un codice di stato HTTP 403 restituito dall'origine e uno restituito da AWS WAF Classic quando una richiesta viene bloccata. Ciò significa che non è possibile restituire pagine di errore personalizzate diverse a seconda delle diverse cause di un codice di stato HTTP 403.

Per ulteriori informazioni sulle pagine di errore CloudFront personalizzate, consulta Customizing Error Responses nella Amazon CloudFront Developer Guide.

Utilizzo di AWS WAF Classic with CloudFront per le applicazioni in esecuzione sul tuo server HTTP

Quando usi AWS WAF Classic con CloudFront, puoi proteggere le tue applicazioni in esecuzione su qualsiasi server Web HTTP, che si tratti di un server Web in esecuzione su Amazon Elastic Compute Cloud (Amazon EC2) o di un server Web gestito privatamente. Puoi anche configurare in modo CloudFront da richiedere HTTPS tra CloudFront e il tuo server web, nonché tra i visualizzatori e. CloudFront

Richiesta di HTTPS tra CloudFront e il proprio server Web

Per richiedere HTTPS tra CloudFront e il tuo server web, puoi utilizzare la funzionalità di origine CloudFront personalizzata e configurare la Origin Protocol Policy e le impostazioni del nome di

dominio di origine per origini specifiche. Nella CloudFront configurazione, è possibile specificare il nome DNS del server insieme alla porta e al protocollo che si desidera utilizzare CloudFront per recuperare oggetti dall'origine. È inoltre necessario assicurarsi che il certificato SSL/TLS sul server di origine personalizzato corrisponda al nome di dominio di origine configurato. Quando si utilizza il proprio server web HTTP all'esterno di AWS, è necessario utilizzare un certificato firmato da un'autorità di certificazione (CA) di terze parti affidabile, ad esempio Comodo o Symantec DigiCert. Per ulteriori informazioni sulla richiesta di HTTPS per la comunicazione tra CloudFront e il tuo server web, consulta l'argomento Richiedere HTTPS per la comunicazione tra CloudFront e la tua origine personalizzata nella Amazon CloudFront Developer Guide.

Richiedere HTTPS tra un visualizzatore e CloudFront

Per richiedere HTTPS tra i visualizzatori e CloudFront, puoi modificare la Viewer Protocol Policy per uno o più comportamenti della cache nella tua CloudFront distribuzione. Per ulteriori informazioni sull'utilizzo di HTTPS tra visualizzatori e CloudFront, consulta l'argomento Richiedere HTTPS per la comunicazione tra visualizzatori e CloudFront nella Amazon CloudFront Developer Guide. Puoi anche portare il tuo certificato SSL in modo che gli spettatori possano connettersi alla tua CloudFront distribuzione tramite HTTPS utilizzando il tuo nome di dominio, ad esempio https://www.mysite.com. Per ulteriori informazioni, consulta l'argomento Configurazione di nomi di dominio alternativi e HTTPS nella Amazon CloudFront Developer Guide.

Scelta dei metodi HTTP che CloudFront rispondono a

Quando crei una distribuzione CloudFront web Amazon, scegli i metodi HTTP che desideri CloudFront elaborare e inoltrare all'origine. Puoi scegliere tra le seguenti opzioni:

- GET, HEAD: puoi utilizzarli CloudFront solo per recuperare oggetti dall'origine o per ottenere le intestazioni degli oggetti.
- GET, HEAD, OPTIONS: è possibile utilizzarli CloudFront solo per recuperare oggetti dall'origine, ottenere le intestazioni degli oggetti o recuperare un elenco delle opzioni supportate dal server di origine.
- GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE: puoi utilizzarli CloudFront per ottenere, aggiungere, aggiornare ed eliminare oggetti e per ottenere le intestazioni degli oggetti. Inoltre, puoi eseguire altre operazioni POST, ad esempio inviare dati da un modulo Web.

È inoltre possibile utilizzare le condizioni di corrispondenza delle stringhe AWS WAF classiche per consentire o bloccare le richieste in base al metodo HTTP, come descritto inUtilizzo di condizioni

di corrispondenza per stringa. Se desideri utilizzare una combinazione di metodi che CloudFront supporti, ad esempio `GET` e`HEAD`, non è necessario configurare AWS WAF Classic per bloccare le richieste che utilizzano gli altri metodi. Se desideri consentire una combinazione di metodi che CloudFront non supporta, ad esempio, e `GET` `HEAD`e`POST`, puoi configurare in modo che CloudFront risponda a tutti i metodi e quindi utilizzare AWS WAF Classic per bloccare le richieste che utilizzano altri metodi.

Per ulteriori informazioni sulla scelta dei metodi a cui CloudFront rispondere, consulta Metodi HTTP consentiti nell'argomento Valori che specifichi quando crei o aggiorni una distribuzione Web nella Amazon CloudFront Developer Guide.

Sicurezza nella AWS WAF versione classica

> **Note**
>
> Questa è la documentazione di AWS WAF Classic. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. L'efficacia della nostra sicurezza è regolarmente testata e verificata da revisori di terze parti come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità applicabili a AWS WAF Classic, consulta AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e leggi e normative applicabili.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi AWS WAF Classic. I seguenti argomenti mostrano come configurare AWS WAF Classic per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse AWS WAF Classic.

Argomenti

Protezione dei dati in AWS WAF Classic

> **Note**
>
> Questa è la documentazione di AWS WAF Classic. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Il modello di responsabilità AWS condivisa modello di si applica alla protezione dei dati in AWS WAF Classic. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal

modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con AWS WAF Classic o altro Servizi AWS utilizzando la console, l'API o gli SDK. AWS CLI AWS I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

AWS WAF Le entità classiche, come gli ACL Web, le regole e le condizioni, sono crittografate quando sono inattive, tranne in alcune regioni in cui la crittografia non è disponibile, tra cui Cina (Pechino) e Cina (Ningxia). Per ogni regione vengono utilizzate chiavi di crittografia univoche.

AWS WAF Eliminazione delle risorse classiche

Puoi eliminare le risorse che crei nella AWS WAF versione classica. Consulta la guida per ogni tipo di risorsa nelle sezioni seguenti.

- Eliminazione di un'ACL Web
- Aggiungere ed eliminare regole da un gruppo di regole AWS WAF classico
- Eliminazione di una regola

Gestione delle identità e degli accessi per AWS WAF Classic

> **Note**
>
> Questa è la documentazione di AWS WAF Classic. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Classic. AWS WAF IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in AWS WAF Classic.

Utente del servizio: se utilizzi il servizio AWS WAF Classic per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità della AWS WAF versione classica per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni

aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità della AWS WAF versione classica, consultaRisoluzione dei problemi relativi all'identità e all'accesso AWS WAF classici.

Amministratore del servizio: se sei responsabile delle risorse di AWS WAF Classic presso la tua azienda, probabilmente hai pieno accesso a AWS WAF Classic. Spetta a te determinare a quali funzionalità e risorse della AWS WAF versione Classic devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con AWS WAF Classic, consultaCome funziona AWS WAF Classic con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso a AWS WAF Classic. Per visualizzare esempi di policy AWS WAF classiche basate sull'identità che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità per Classic AWS WAF

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le

chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.

- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori

informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'azione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruoli IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS.

Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.

- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona AWS WAF Classic con IAM

> **Note**
>
> Questa è la documentazione di AWS WAF Classic. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Prima di utilizzare IAM per gestire l'accesso a AWS WAF Classic, scopri quali funzionalità IAM sono disponibili per l'uso con AWS WAF Classic.

Funzionalità IAM che puoi utilizzare con AWS WAF Classic

Funzionalità IAM	AWS WAF Supporto classico
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come AWS WAF Classic e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per Classic AWS WAF

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Per visualizzare esempi di politiche AWS WAF classiche basate sull'identità, vedere. Esempi di policy basate sull'identità per Classic AWS WAF

Politiche basate sulle risorse all'interno di Classic AWS WAF

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Azioni politiche per AWS WAF Classic

Supporta le azioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di azioni AWS WAF classiche, vedere Azioni definite da AWS WAF e Azioni definite da AWS WAF Regional nel Service Authorization Reference.

Le azioni politiche in AWS WAF Classic utilizzano il seguente prefisso prima dell'azione:

```
waf
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "waf:action1",
      "waf:action2"
         ]
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni in AWS WAF Classic che iniziano con`List`, includi la seguente azione:

```
"Action": "waf:List*"
```

Per visualizzare esempi di politiche AWS WAF classiche basate sull'identità, vedere. Esempi di policy basate sull'identità per Classic AWS WAF

Risorse politiche per Classic AWS WAF

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare l'elenco dei tipi di risorse AWS WAF Classic e dei relativi ARN, vedere Resources defined by AWS WAF e Resources defined by AWS WAF Regional nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, vedere Azioni definite da AWS WAF e Azioni definite da Regional. AWS WAF Per consentire o negare l'accesso a un sottoinsieme di risorse AWS WAF Classic, includi l'ARN della risorsa nell'`resource`elemento della tua politica.

Nella AWS WAF versione classica, le risorse sono ACL e regole Web. AWS WAF La versione classica supporta anche condizioni quali la corrispondenza tra byte, la corrispondenza IP e il vincolo di dimensione.

A queste risorse e a queste condizioni sono associati Amazon Resource Name (ARN) univoci, come mostrato nella tabella seguente.

Nome nella console AWS WAF	Nome in AWS WAF SDK/CLI	Formato ARN
ACL Web	`WebACL`	`arn:aws:waf:: account:webacl/ID`
Regola	`Rule`	`arn:aws:waf:: account:rule/ID`
Condizione di corrispondenza stringa	`ByteMatch Set`	`arn:aws:waf:: account:bytematch set /ID`

Nome nella console AWS WAF	Nome in AWS WAF SDK/CLI	Formato ARN
condizione di corrispondenza SQL injection	`SqlInjectionMatchSet`	`arn:aws:waf::` *`account`*`:sqlinjectionset /`*`ID`
Condizione di vincolo di dimensione	`SizeConstraintSet`	`arn:aws:waf::` *`account`*`:sizeconstraintset /`*`ID`
Condizione di corrispondenza IP	`IPSet`	`arn:aws:waf::` *`account`*`:ipset/`*`ID`
Condizione di corrispondenza Cross-site scripting	`XssMatchSet`	`arn:aws:waf::` *`account`*`:xssmatchset /`*`ID`

Per consentire o negare l'accesso a un sottoinsieme di risorse AWS WAF Classic, includi l'ARN della risorsa nell'`resource`elemento della tua politica. Gli ARN per AWS WAF Classic hanno il seguente formato:

```
arn:aws:waf::account:resource/ID
```

Sostituisci le variabili *`account`*, *`resource`* e *`ID`* con valori validi. I valori validi possono essere i seguenti:

- *`account`*: l'ID del tuo Account AWS. È necessario specificare un valore.
- *`risorsa`*: il tipo di risorsa AWS WAF classica.
- *`ID`*: l'ID della risorsa AWS WAF classica o un carattere jolly (*) per indicare tutte le risorse del tipo specificato associate alla risorsa specificata Account AWS.

Ad esempio, il seguente ARN specifica tutte le ACL Web per l'account `111122223333`:

```
arn:aws:waf::111122223333:webacl/*
```

Chiavi relative alle condizioni della policy per Classic AWS WAF

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco delle chiavi di condizione AWS WAF classiche, consulta Chiavi di condizione per AWS WAF e Risorse definite da AWS WAF Regional nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, vedi Azioni definite da AWS WAF e Azioni definite da AWS WAF Regional.

Per visualizzare esempi di politiche AWS WAF classiche basate sull'identità, vedere. Esempi di policy basate sull'identità per Classic AWS WAF

ACL nella versione classica AWS WAF

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con Classic AWS WAF

Supporta ABAC (tag nelle policy)	Parziale

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Classic AWS WAF

Supporta le credenziali temporanee	Sì

Alcune Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Sessioni di accesso diretto per Classic AWS WAF

Supporta sessioni di accesso diretto (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

Ruoli di servizio per Classic AWS WAF

Supporta i ruoli di servizio	Sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità AWS WAF Classic. Modifica i ruoli di servizio solo quando AWS WAF Classic fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per Classic AWS WAF

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione dei ruoli AWS WAF classici collegati ai servizi, consulta. Utilizzo di ruoli collegati ai servizi per Classic AWS WAF

Esempi di policy basate sull'identità per Classic AWS WAF

> **Note**
>
> Questa è la documentazione di Classic AWS WAF . Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse AWS WAF Classic. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS l'API. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da AWS WAF Classic, incluso il formato degli ARN per ciascun tipo di risorsa, vedere Azioni, risorse e chiavi di condizione per e Azioni, risorse AWS WAF e chiavi di condizione per AWS WAF Regional nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console Classic AWS WAF
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse AWS WAF Classic nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso ad azioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Classic AWS WAF

Per accedere alla console AWS WAF Classic, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse della AWS WAF versione classica del tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Gli utenti che possono accedere e utilizzare la AWS console possono accedere anche alla console AWS WAF Classic. Non sono necessarie autorizzazioni supplementari.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questo criterio include le autorizzazioni per completare questa azione sulla console o a livello di codice utilizzando l' AWS CLI API 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": "*"
        }
    ]
}
```

Risoluzione dei problemi relativi all'identità e all'accesso AWS WAF classici

> **Note**
>
> Questa è la documentazione della AWS WAF versione classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF. Per la versione più recente di AWS WAF, vedi. AWS WAF

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con AWS WAF Classic e IAM.

Argomenti

Non sono autorizzato a eseguire un'azione in Classic AWS WAF

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `waf:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 waf:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `waf:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di passare un ruolo a AWS WAF Classic.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in AWS WAF Classic. Tuttavia, l'azione richiede che

il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Desidero consentire a persone esterne Account AWS a me di accedere alle mie risorse AWS WAF Classic

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS WAF Classic supporta queste funzionalità, consultaCome funziona AWS WAF Classic con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Utilizzo di ruoli collegati ai servizi per Classic AWS WAF

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

AWS WAF La versione classica utilizza AWS Identity and Access Management ruoli collegati ai servizi (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a Classic. AWS WAF I ruoli collegati ai servizi sono predefiniti da AWS WAF Classic e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato ai servizi semplifica la configurazione di AWS WAF Classic perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS WAF Classic definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo AWS WAF Classic può assumerne i ruoli. Le autorizzazioni definite includono policy di attendibilità e di autorizzazioni. Questa policy delle autorizzazioni non può essere collegata ad alcun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. In questo modo proteggi le tue risorse AWS WAF Classic perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate al servizio per Classic AWS WAF

AWS WAF Classic utilizza i seguenti ruoli collegati ai servizi:

- `AWSServiceRoleForWAFLogging`
- `AWSServiceRoleForWAFRegionalLogging`

AWS WAF Classic utilizza questi ruoli collegati ai servizi per scrivere log su Amazon Data Firehose. Questi ruoli vengono utilizzati solo se abiliti l'accesso. AWS WAF Per ulteriori informazioni, consulta Registrazione informazioni di traffico ACL Web.

I ruoli `AWSServiceRoleForWAFRegionalLogging` collegati ai servizi `AWSServiceRoleForWAFLogging` e affidano il ruolo ai seguenti servizi (rispettivamente):

- `waf.amazonaws.com`

  `waf-regional.amazonaws.com`

Le politiche di autorizzazione dei ruoli consentono a AWS WAF Classic di completare le seguenti azioni sulle risorse specificate:

- Azione: `firehose:PutRecord` e `firehose:PutRecordBatch` su Amazon Data Firehose risorse di flusso di dati con un nome che inizia con "aws-waf-logs-». Ad esempio, `aws-waf-logs-us-east-2-analytics`.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Classic AWS WAF

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando abiliti l'accesso AWS WAF classico o AWS Management Console effettui una `PutLoggingConfiguration` richiesta nella CLI AWS WAF classica o nell'API classica AWS WAF , Classic crea automaticamente AWS WAF il ruolo collegato al servizio.

È necessario disporre dell'autorizzazione `iam:CreateServiceLinkedRole` per attivare la registrazione.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando abiliti la registrazione AWS WAF classica, AWS WAF Classic crea nuovamente il ruolo collegato al servizio per te.

Modifica di un ruolo collegato al servizio per Classic AWS WAF

AWS WAF La versione classica non consente di modificare i ruoli collegati al `AWSServiceRoleForWAFLogging` `AWSServiceRoleForWAFRegionalLogging` servizio. Dopo

aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Classic AWS WAF

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

> **Note**
>
> Se il servizio AWS WAF Classic utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse AWS WAF Classic utilizzate da **`AWSServiceRoleForWAFLogging`** e **`AWSServiceRoleForWAFRegionalLogging`**

1. Sulla console AWS WAF Classic, rimuovi la registrazione da ogni ACL Web. Per ulteriori informazioni, consulta Registrazione informazioni di traffico ACL Web.
2. Utilizzando l'API o l'interfaccia CLI, inviare una richiesta di `DeleteLoggingConfiguration` per ogni ACL Web che ha la registrazione attivata. Per ulteriori informazioni, consulta AWS WAF Classic API Reference.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM, l'IAM CLI o l'API IAM per eliminare i ruoli `AWSServiceRoleForWAFLogging` e i ruoli collegati ai `AWSServiceRoleForWAFRegionalLogging` servizi. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli classici collegati ai servizi AWS WAF

AWS WAF La versione classica supporta l'utilizzo di ruoli collegati ai servizi nei seguenti casi. Regioni AWS

Nome della regione	Identità della regione	Support nella AWS WAF versione classica
Stati Uniti orientali (Virginia settentri onale)	us-east-1	Sì
Stati Uniti orientali (Ohio)	us-east-2	Sì
Stati Uniti occidentali (California settentri onale)	us-west-1	Sì
US West (Oregon)	us-west-2	Sì
Asia Pacifico (Mumbai)	ap-south-1	Sì
Asia Pacifico (Osaka-Locale)	ap-northeast-3	Sì
Asia Pacifico (Seul)	ap-northeast-2	Sì
Asia Pacifico (Singapore)	ap-southeast-1	Sì
Asia Pacifico (Sydney)	ap-southeast-2	Sì
Asia Pacifico (Tokyo)	ap-northeast-1	Sì
Canada (Centrale)	ca-central-1	Sì
Europa (Francoforte)	eu-central-1	Sì
Europa (Irlanda)	eu-west-1	Sì
Europa (Londra)	eu-west-2	Sì
Europa (Parigi)	eu-west-3	Sì
Sud America (San Paolo)	sa-east-1	Sì

Registrazione e monitoraggio nella versione classica AWS WAF

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di AWS WAF Classic e delle tue AWS soluzioni. È necessario raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica uno. AWS offre diversi strumenti per monitorare le risorse AWS WAF Classic e rispondere a potenziali eventi:

CloudWatch Allarmi Amazon

Utilizzando gli CloudWatch allarmi, controlli una singola metrica per un periodo di tempo specificato. Se la metrica supera una determinata soglia, CloudWatch invia una notifica a un argomento o una policy di Amazon SNS. AWS Auto Scaling Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch.

AWS CloudTrail Registri

CloudTrail fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in AWS WAF Classic. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta che è stata effettuata a AWS WAF Classic, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli. Per ulteriori informazioni, consulta Registrazione delle chiamate API di AWS CloudTrail con.

Convalida della conformità per Classic AWS WAF

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive come le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

  > **Note**
  >
  > Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e

mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).

- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente AWS l'utilizzo per semplificare la gestione dei rischi e la conformità alle normative e agli standard di settore.

Resilienza nella versione classica AWS WAF

> **Note**
>
> Questa è la documentazione di Classic AWS WAF . Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

Sicurezza dell'infrastruttura in AWS WAF Classic

> **Note**
>
> Questa è la documentazione di AWS WAF Classic. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

In quanto servizio gestito, AWS WAF Classic è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere a AWS WAF Classic tramite la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

AWS WAF Quote classiche

> **Note**
>
> Questa è la documentazione AWS WAF classica. Dovresti usare questa versione solo se hai creato AWS WAF risorse, come regole e ACL web, AWS WAF prima di novembre 2019 e non le hai ancora migrate alla versione più recente. Per eseguire la migrazione delle risorse, consulta Migrazione delle risorse AWS WAF Classic a AWS WAF.
> Per la versione più recente di AWS WAF, vedi. AWS WAF

AWS WAF Classic è soggetto alle seguenti quote (precedentemente denominate limiti).

AWS WAF Classic ha quote predefinite sul numero di entità per account per regione. È possibile richiedere un aumento delle quote.

Risorsa	Quota predefinita per account per regione
ACL Web	50
Regole	100
R ate-based-rules	5
Condizioni per account per regione	Per tutte le condizioni tranne

Risorsa	Quota predefinita per account per regione
	regex match e geo match, 100 per ogni tipo di condizione. Ad esempio, 100 condizioni di vincolo di dimensione e 100 condizioni di corrispondenza IP. Per le condizioni di regex e geo match, consultate la tabella seguente.
Richieste al secondo	25.000 per lista di controllo degli accessi Web*

*Questa quota si applica solo a AWS WAF Classic on an Application Load Balancer. Le quote RPS (Requests per Second) per AWS WAF Classic on CloudFront sono le stesse supportate per le quote RPS, descritte nella Developer CloudFront Guide. CloudFront

Le seguenti quote sulle entità AWS WAF Classic non possono essere modificate.

Risorsa	Quota per account per regione
Gruppi di regole per ACL Web	2:1 gruppo di regole creato

Risorsa	Quota per account per regione
	dal cliente e 1 gruppo di regole Marketplace AWS
Regole per lista di controllo degli accessi Web	10
Condizioni per regola	10
Intervalli di indirizzi IP (in notazione CIDR) per condizione di corrispondenza IP	10.000 Puoi aggiornare fino a 1.000 indirizzi alla volta. La chiamata API `UpdateIPSet` accetta un massimo di 1.000 indirizzi in una singola richiesta.
Indirizzi IP bloccati per ogni regola basata sulla frequenza	10.000
Limite frequenza della regola basata sulla frequenza minima per un periodo di 5 minuti	100
Filtri per condizione di corrispondenza Cross-site scripting	10
Filtri per condizione di vincolo di dimensione	10
Filtri per condizione di corrispondenza SQL injection	10
Filtri per condizione di corrispondenza stringa	10

Risorsa	Quota per account per regione
In condizioni di corrispondenza delle stringhe, il numero di caratteri nei nomi delle intestazioni HTTP, se hai configurato AWS WAF Classic per controllare le intestazioni nelle richieste Web alla ricerca di un valore specificato	40
In condizioni di corrispondenza delle stringhe, il numero di caratteri del valore che vuoi che AWS WAF Classic cerchi	50
Condizioni di corrispondenza Regex	10
Nelle condizioni di corrispondenza regex, il numero di caratteri del pattern che AWS WAF Classic deve cercare	70
Nelle condizioni di corrispondenza regex, il numero di modelli per ogni set di modelli	10
Nelle condizioni di corrispondenza regex, il numero di set del modello per ogni condizione regex	1
Set di pattern	5
Condizioni di geo-match	50
Posizioni per condizione di corrispondenza geografica	50

AWS WAF Classic ha le seguenti quote fisse di chiamate per account per regione. Queste quote si applicano al totale delle chiamate al servizio tramite qualsiasi mezzo disponibile, tra cui la console, la CLI AWS CloudFormation, l'API REST e gli SDK. Queste quote non possono essere modificate.

Tipo di chiamata	Quota per account per regione
Numero massimo di chiamate a `AssociateWebACL`	1 richiesta ogni 2 secondi

Tipo di chiamata	Quota per account per regione
Numero massimo di chiamate a `DisassociateWebACL`	1 richiesta ogni 2 secondi
Numero massimo di chiamate a `GetWebACLForResource`	1 richiesta al secondo
Numero massimo di chiamate a `ListResourcesForWebACL`	1 richiesta al secondo
Numero massimo di chiamate a `CreateWebACLMigrationStack`	1 richiesta al secondo
Numero massimo di chiamate a `GetChangeToken`	10 richieste al secondo
Numero massimo di chiamate a `GetChangeTokenStatus`	1 richiesta al secondo
Numero massimo di chiamate a qualsiasi operazione singola `List`, se per l'operazione non è definita una quota diversa	5 richieste al secondo
Numero massimo di chiamate a qualsiasi operazione singola `Create`, `Put`, `Get` o `Update`, se per l'operazione non è definita una quota diversa	1 richiesta al secondo

AWS Shield

La protezione dagli attacchi Distributed Denial of Service (DDoS) è di primaria importanza per le applicazioni connesse a Internet. Quando costruisci la tua applicazione AWS, puoi utilizzare le protezioni fornite senza costi aggiuntivi. AWS Inoltre, è possibile utilizzare il servizio AWS Shield Advanced gestito di protezione dalle minacce per migliorare il livello di sicurezza con funzionalità aggiuntive di rilevamento, mitigazione e risposta agli attacchi DDoS.

AWS si impegna a fornirti gli strumenti, le migliori pratiche e i servizi per contribuire a garantire disponibilità, sicurezza e resilienza elevate nella tua difesa contro i malintenzionati su Internet. Questa guida viene fornita per aiutare i responsabili delle decisioni IT e gli ingegneri della sicurezza a capire come utilizzare Shield e Shield Advanced per proteggere meglio le loro applicazioni dagli attacchi DDoS e da altre minacce esterne.

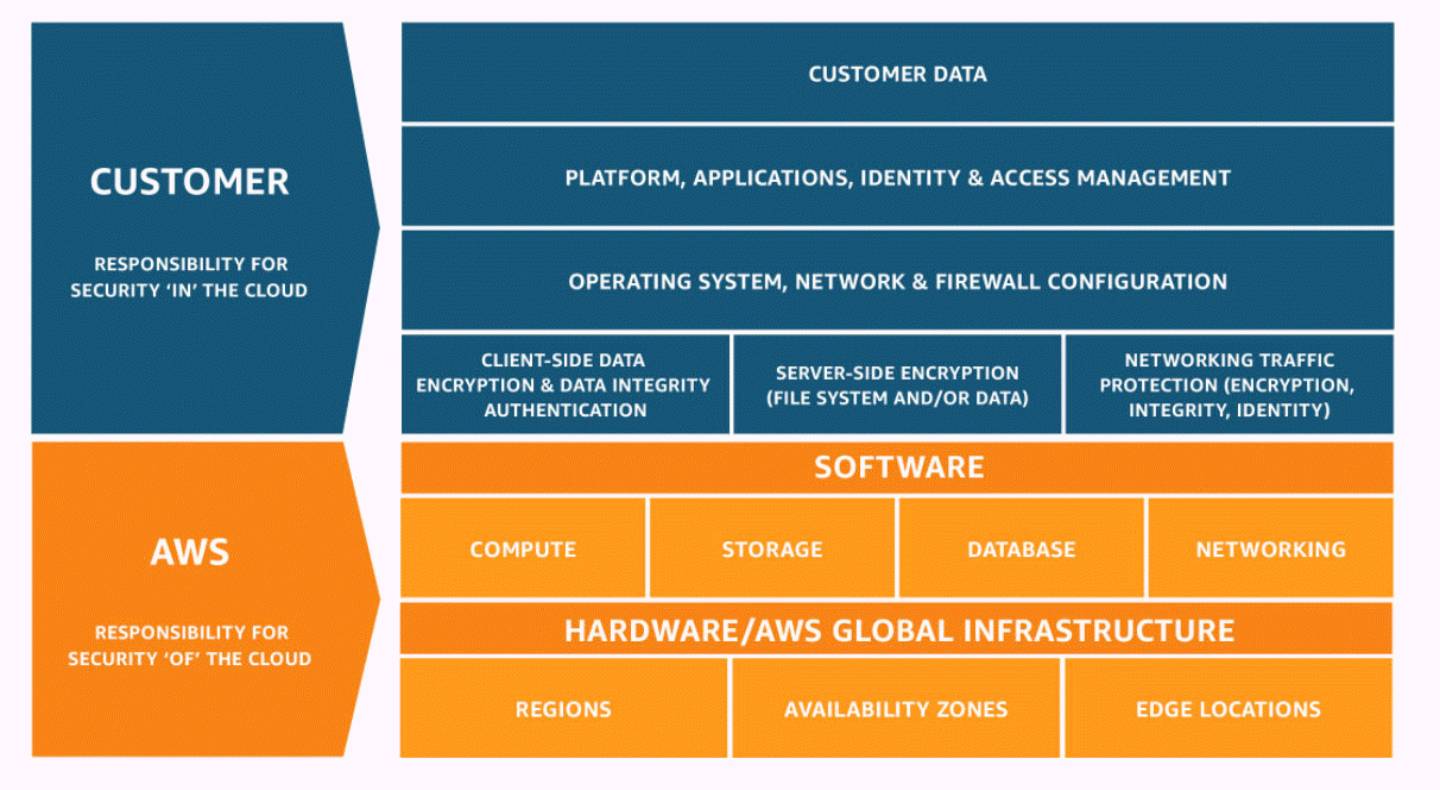
Quando costruisci la tua applicazione AWS, ricevi una protezione automatica AWS contro i comuni vettori di attacco DDoS volumetrici, come gli attacchi di riflessione UDP e i flood TCP SYN. Puoi sfruttare queste protezioni per garantire la disponibilità delle applicazioni su cui esegui progettando e configurando l'architettura per la resilienza DDoS. AWS

Questa guida fornisce consigli che possono aiutarti a progettare, creare e configurare architetture applicative per la resilienza DDoS. Le applicazioni che aderiscono alle migliori pratiche fornite in questa guida possono trarre vantaggio da una maggiore continuità di disponibilità quando sono prese di mira da attacchi DDoS più ampi e da una gamma più ampia di vettori di attacco DDoS. Inoltre, questa guida mostra come utilizzare Shield Advanced per implementare una posizione di protezione DDoS ottimizzata per le applicazioni critiche. Queste includono le applicazioni per le quali hai garantito un certo livello di disponibilità ai tuoi clienti e quelle che richiedono supporto operativo AWS durante gli eventi DDoS.

La sicurezza è una responsabilità condivisa tra te AWS e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. L'efficacia della nostra sicurezza è regolarmente testata e verificata da revisori di terze parti come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità che si applicano a Shield Advanced, consulta AWS Services in Scope by Compliance Program.

- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e leggi e normative applicabili.



Come funzionano AWS Shield e Shield Advanced

AWS Shield Standard e AWS Shield Advanced forniscono protezioni contro gli attacchi DDoS (Distributed Denial of Service) per AWS le risorse a livello di rete e trasporto (livelli 3 e 4) e a livello di applicazione (livello 7). Un attacco DDoS è un attacco in cui più sistemi compromessi cercano di inondare di traffico un bersaglio. Un attacco DDoS può impedire agli utenti finali legittimi di accedere ai servizi bersaglio e può causare il blocco dell'obiettivo a causa dell'eccessivo volume di traffico.

AWS Shield fornisce protezione contro un'ampia gamma di vettori di attacco DDoS e vettori di attacco zero-day noti. Il rilevamento e la mitigazione dello Shield sono progettati per fornire copertura contro le minacce anche se non sono note esplicitamente al servizio al momento del rilevamento. Shield Standard viene fornito automaticamente e senza costi aggiuntivi durante l'uso AWS.

Le classi di attacchi rilevate da Shield includono le seguenti:

- Attacchi volumetrici di rete (livello 3): si tratta di una sottocategoria dei vettori di attacco a livello di infrastruttura. Questi vettori tentano di saturare la capacità della rete o della risorsa bersaglio, di negare il servizio agli utenti legittimi.
- Attacchi al protocollo di rete (livello 4): si tratta di una sottocategoria dei vettori di attacco a livello di infrastruttura. Questi vettori abusano di un protocollo per negare il servizio alla risorsa bersaglio. Un esempio comune di attacco al protocollo di rete è il TCP SYN flood, che può esaurire lo stato della connessione su risorse come server, sistemi di bilanciamento del carico o firewall. Un attacco al protocollo di rete può anche essere volumetrico. Ad esempio, un TCP SYN flood più ampio può avere l'obiettivo di saturare la capacità di una rete e allo stesso tempo di esaurire lo stato della risorsa o delle risorse intermedie prese di mira.
- Attacchi a livello applicativo (livello 7): questa categoria di vettori di attacco tenta di negare il servizio agli utenti legittimi inondando un'applicazione di query valide per l'obiettivo, come i flussi di richieste Web.

Indice

AWS Shield Standard panoramica

AWS Shield è un servizio gestito di protezione dalle minacce che protegge il perimetro dell'applicazione. Il perimetro è il primo punto di ingresso per il traffico delle applicazioni proveniente dall'esterno della rete. AWS

Per determinare dove si trova il perimetro dell'applicazione, considerate in che modo gli utenti accedono all'applicazione da Internet. Se il primo punto di ingresso si trova in una AWS regione, il perimetro dell'applicazione è Amazon Virtual Private Cloud (VPC). Se gli utenti vengono indirizzati alla tua applicazione da Amazon Route 53 e accedono per la prima volta all'applicazione tramite Amazon CloudFront o AWS Global Accelerator, il perimetro dell'applicazione inizia ai margini della AWS rete.

Shield offre vantaggi di rilevamento e mitigazione degli attacchi DDoS per tutte le applicazioni in esecuzione AWS, ma le decisioni prese durante la progettazione dell'architettura dell'applicazione influenzeranno il livello di resilienza DDoS. La resilienza DDoS è la capacità dell'applicazione di continuare a funzionare entro i parametri previsti durante un attacco.

Tutti AWS i clienti beneficiano della protezione automatica di Shield Standard, senza costi aggiuntivi. Shield Standard difende dagli attacchi DDoS più comuni e frequenti a livello di rete e trasporto che prendono di mira il tuo sito Web o le tue applicazioni. Sebbene Shield Standard aiuti a proteggere tutti AWS i clienti, ottieni vantaggi particolari con le zone ospitate di Amazon Route 53, CloudFront le distribuzioni Amazon e gli AWS Global Accelerator acceleratori standard. Queste risorse ricevono una protezione completa della disponibilità contro tutti gli attacchi noti a livello di rete e trasporto.

AWS Shield Advanced panoramica

AWS Shield Advanced è un servizio gestito che consente di proteggere l'applicazione da minacce esterne, come attacchi DDoS, bot volumetrici e tentativi di sfruttamento delle vulnerabilità. Per livelli più elevati di protezione contro gli attacchi, puoi effettuare la sottoscrizione ad AWS Shield Advanced.

Quando ti abboni a Shield Advanced e aggiungi protezione alle tue risorse, Shield Advanced offre una protezione estesa dagli attacchi DDoS per tali risorse. Le protezioni che ricevi da Shield Advanced possono variare a seconda dell'architettura e delle scelte di configurazione. Utilizza le informazioni contenute in questa guida per creare e proteggere applicazioni resilienti utilizzando Shield Advanced e per aumentare la richiesta quando hai bisogno dell'aiuto di un esperto.

Abbonamenti e AWS WAF costi Shield Advanced

L'abbonamento a Shield Advanced copre i costi di utilizzo delle AWS WAF funzionalità standard per le risorse che proteggi con Shield Advanced. AWS WAF Le tariffe standard coperte dalle protezioni Shield Advanced sono il costo per ACL Web, il costo per regola e il prezzo base per milione di richieste per l'ispezione delle richieste Web, fino a 1.500 WCU e fino alla dimensione corporea predefinita.

L'attivazione della mitigazione automatica degli attacchi DDoS a livello di applicazione Shield Advanced aggiunge un gruppo di regole all'ACL Web che utilizza 150 unità di capacità ACL Web (WCU). Queste WCU influiscono sull'utilizzo della WCU nell'ACL web. Per ulteriori informazioni, consulta Mitigazione DDoS automatica a livello di applicazione Shield Advanced, Il gruppo di regole Shield Advanced e AWS WAF unità di capacità Web ACL (WCU).

L'abbonamento a Shield Advanced non copre l'uso AWS WAF di risorse che non proteggi utilizzando Shield Advanced. Inoltre, non copre eventuali AWS WAF costi aggiuntivi non standard per le risorse protette. Esempi di AWS WAF costi non standard sono quelli per Bot Control, per l'azione delle CAPTCHA regole, per gli ACL Web che utilizzano più di 1.500 WCU e per l'ispezione del corpo della richiesta oltre le dimensioni corporee predefinite. L'elenco completo è disponibile nella pagina dei prezzi. AWS WAF

Per informazioni complete ed esempi di prezzi, consulta la pagina Prezzi e AWS WAF prezzi di Shield.

Fatturazione dell'abbonamento Shield Advanced

Se sei un AWS Channel Reseller, contatta il team del tuo account per informazioni e assistenza. Queste informazioni di fatturazione sono destinate ai clienti che non sono rivenditori di AWS canale.

Per tutti gli altri, si applicano le seguenti linee guida per l'abbonamento e la fatturazione:

- Per gli account membri di un' AWS Organizations organizzazione, AWS addebita gli abbonamenti Shield Advanced sul conto pagante dell'organizzazione, indipendentemente dal fatto che l'account di pagamento stesso sia sottoscritto.
- Quando sottoscrivi più account appartenenti alla stessa famiglia di conti di fatturazione AWS Organizations consolidati, un unico prezzo di abbonamento copre tutti gli account sottoscritti della famiglia. L'organizzazione deve possedere tutte Account AWS e tutte le proprie risorse.
- Quando sottoscrivi più account per più organizzazioni, puoi comunque pagare un'unica quota di abbonamento per tutte le organizzazioni, gli account e le risorse, purché tu ne sia il proprietario. Contatta il tuo account manager o l' AWS assistenza e richiedi un'esenzione dai costi di AWS Shield Advanced abbonamento per tutte le organizzazioni tranne una.

Per informazioni dettagliate ed esempi sui prezzi, consulta AWS Shield Prezzi.

Argomenti

AWS Shield Advanced risorse protette

> **Note**
>
> Le protezioni Shield Advanced sono abilitate solo per le risorse che hai specificato esplicitamente in Shield Advanced o che proteggi tramite una politica AWS Firewall Manager Shield Advanced. Shield Advanced non protegge automaticamente le tue risorse.

È possibile utilizzare Shield Advanced per il monitoraggio e la protezione avanzati con i seguenti tipi di risorse:

- CloudFront Distribuzioni Amazon. Per la distribuzione CloudFront continua, Shield Advanced protegge qualsiasi distribuzione temporanea associata a una distribuzione primaria protetta.
- Zone ospitate Amazon Route 53.
- AWS Global Accelerator acceleratori standard.
- Indirizzi IP elastici di Amazon EC2. Shield Advanced protegge le risorse associate agli indirizzi IP elastici protetti.
- Istanze Amazon EC2, tramite associazione a indirizzi IP elastici di Amazon EC2.
- I seguenti sistemi di bilanciamento del carico Elastic Load Balancing (ELB):
  - Application Load Balancer.
  - Classic Load Balancer.
  - Network Load Balancer, tramite associazioni agli indirizzi IP elastici di Amazon EC2.

Per ulteriori informazioni sulle protezioni per questi tipi di risorse, consulta. AWS Shield Advanced protezioni per tipo di risorsa

AWS Shield Advanced funzionalità e opzioni

AWS Shield Advanced l'abbonamento include le seguenti funzionalità e opzioni. Queste funzionalità integrano le funzionalità di rilevamento e mitigazione degli attacchi DDoS già incluse. AWS

- AWS WAF integrazione: Shield Advanced utilizza ACL AWS WAF Web, regole e gruppi di regole come parte delle sue protezioni a livello di applicazione. Per ulteriori informazioni su AWS WAF, vedere. Come AWS WAF funziona

  > **Note**
  >
  > L'abbonamento a Shield Advanced copre i costi di utilizzo delle AWS WAF funzionalità standard per le risorse che proteggi con Shield Advanced. AWS WAF Le tariffe standard coperte dalle protezioni Shield Advanced sono il costo per ACL Web, il costo per regola e il prezzo base per milione di richieste per l'ispezione delle richieste Web, fino a 1.500 WCU e fino alla dimensione corporea predefinita.
  >
  > L'attivazione della mitigazione automatica degli attacchi DDoS a livello di applicazione Shield Advanced aggiunge un gruppo di regole all'ACL Web che utilizza 150 unità di capacità ACL Web (WCU). Queste WCU influiscono sull'utilizzo della WCU nell'ACL web. Per ulteriori informazioni, consulta Mitigazione DDoS automatica a livello di applicazione Shield Advanced, Il gruppo di regole Shield Advanced e AWS WAF unità di capacità Web ACL (WCU).
  >
  > L'abbonamento a Shield Advanced non copre l'uso AWS WAF di risorse che non proteggi utilizzando Shield Advanced. Inoltre, non copre eventuali AWS WAF costi aggiuntivi non standard per le risorse protette. Esempi di AWS WAF costi non standard sono quelli per Bot Control, per l'azione delle CAPTCHA regole, per gli ACL Web che utilizzano più di 1.500 WCU e per l'ispezione del corpo della richiesta oltre le dimensioni corporee predefinite. L'elenco completo è disponibile nella pagina dei prezzi. AWS WAF
  >
  > Per informazioni complete ed esempi di prezzi, consulta la pagina Prezzi e AWS WAF prezzi di Shield.

- Mitigazione automatica degli attacchi DDoS a livello di applicazione: puoi configurare Shield Advanced per rispondere automaticamente e mitigare gli attacchi a livello di applicazione (livello 7) contro le tue risorse protette. Con la mitigazione automatica, Shield Advanced impone la limitazione della AWS WAF velocità sulle richieste provenienti da fonti DDoS note e aggiunge e gestisce automaticamente AWS WAF protezioni personalizzate in risposta agli attacchi DDoS rilevati. È possibile configurare la mitigazione automatica per contare o bloccare le richieste Web che fanno parte di un attacco.

Per ulteriori informazioni, consulta Mitigazione DDoS automatica a livello di applicazione Shield Advanced.

- Rilevamento basato sullo stato: puoi utilizzare i controlli dello stato di Amazon Route 53 con Shield Advanced per rilevare e mitigare gli eventi in modo mirato. I controlli sanitari monitorano l'applicazione in base alle specifiche, segnalando lo stato di integrità quando le specifiche sono soddisfatte e lo stato non lo è quando non lo sono. L'utilizzo dei controlli di integrità con Shield Advanced aiuta a prevenire i falsi positivi e fornisce un rilevamento e una mitigazione più rapidi quando una risorsa protetta non è integra. È possibile utilizzare il rilevamento basato sullo stato di salute per qualsiasi tipo di risorsa ad eccezione delle zone ospitate su Route 53. Il coinvolgimento proattivo Shield Advanced è disponibile solo per le risorse che hanno abilitato il rilevamento basato sullo stato di salute.

  Per ulteriori informazioni, consulta Rilevamento basato sulla salute mediante controlli sanitari.

- Gruppi di protezione: è possibile utilizzare i gruppi di protezione per creare raggruppamenti logici delle risorse protette, per migliorare il rilevamento e la mitigazione del gruppo nel suo insieme. È possibile definire i criteri per l'appartenenza a un gruppo di protezione in modo che le nuove risorse protette vengano incluse automaticamente. Una risorsa protetta può appartenere a più gruppi di protezione.

  Per ulteriori informazioni, consulta AWS Shield Advanced gruppi di protezione.

- Visibilità migliorata su eventi e attacchi DDoS: Shield Advanced ti dà accesso a metriche e report avanzati in tempo reale per una visibilità completa su eventi e attacchi alle tue risorse protette AWS . Puoi accedere a queste informazioni tramite l'API e la console Shield Advanced e tramite Amazon CloudWatch metrics.

  Per ulteriori informazioni, consulta Visibilità sugli eventi DDoS.

- Gestione centralizzata delle protezioni Shield Advanced tramite AWS Firewall Manager: puoi utilizzare Firewall Manager per applicare automaticamente le protezioni Shield Advanced ai tuoi nuovi account e risorse e per distribuire AWS WAF regole agli ACL web. Le policy di protezione Firewall Manager Shield Advanced sono incluse senza costi aggiuntivi per i clienti di Shield Advanced. Puoi anche centralizzare le attività di monitoraggio Shield Advanced per i tuoi account utilizzando Firewall Manager con un argomento Amazon Simple Notification Service (SNS) oppure. AWS Security Hub

Per ulteriori informazioni sull'utilizzo di Firewall Manager per gestire le protezioni Shield Advanced, vedere AWS Firewall Manager eAWS Shield Advanced politiche. Per informazioni sui prezzi di Firewall Manager, consulta AWS Firewall Manager Prezzi.

- AWS Shield Response Team (SRT) — L'SRT ha una vasta esperienza nella protezione AWS di Amazon.com e delle sue filiali. In qualità di AWS Shield Advanced cliente, puoi contattare l'SRT in qualsiasi momento per ricevere assistenza durante un attacco DDoS che influisce sulla disponibilità dell'applicazione. Puoi anche collaborare con SRT per creare e gestire mitigazioni personalizzate per le tue risorse. Per utilizzare i servizi dell'SRT, è inoltre necessario essere abbonati al piano Business Support o al piano Enterprise Support.

  Per ulteriori informazioni, consulta Supporto dello Shield Response Team (SRT).
- Coinvolgimento proattivo: con il coinvolgimento proattivo, lo Shield Response Team (SRT) ti contatta direttamente se il controllo dello stato di Amazon Route 53 che hai associato alla tua risorsa protetta non funziona correttamente durante un evento rilevato da Shield Advanced. In questo modo puoi interagire più rapidamente con gli esperti quando la disponibilità dell'applicazione potrebbe essere compromessa da un attacco sospetto.

  Per ulteriori informazioni, consulta Configurazione del coinvolgimento proattivo.
- Opportunità di protezione dei costi: Shield Advanced offre una certa protezione dai picchi di AWS bolletta che potrebbero derivare da un attacco DDoS contro le risorse protette. Ciò può includere la copertura per i picchi delle tariffe di utilizzo di Shield Advanced data transfer out (DTO). Shield Advanced fornisce qualsiasi protezione dei costi sotto forma di crediti di servizio Shield Advanced.

  Per ulteriori informazioni, consulta Richiedere un credito in AWS Shield Advanced.

Decidere se abbonarsi AWS Shield Advanced e applicare protezioni aggiuntive

Consulta gli scenari in questa sezione per aiutarti a decidere a quali account abbonarti AWS Shield Advanced e dove applicare protezioni aggiuntive. Con Shield Advanced, paghi una quota di abbonamento mensile per tutti gli account creati con un account di fatturazione consolidato, più le tariffe di utilizzo basate su GB di dati trasferiti in uscita. Per informazioni sui prezzi di Shield Advanced, consulta AWS Shield Advanced Prezzi.

Per proteggere un'applicazione e le relative risorse con Shield Advanced, sottoscrivi gli account che gestiscono l'applicazione a Shield Advanced e quindi aggiungi protezioni alle risorse dell'applicazione. Per informazioni sulla sottoscrizione degli account e sulla protezione delle risorse, consulta. Iniziare con AWS Shield Advanced

Abbonamenti e AWS WAF costi Shield Advanced

L'abbonamento a Shield Advanced copre i costi di utilizzo delle AWS WAF funzionalità standard per le risorse che proteggi con Shield Advanced. AWS WAF Le tariffe standard coperte dalle protezioni Shield Advanced sono il costo per ACL Web, il costo per regola e il prezzo base per milione di richieste per l'ispezione delle richieste Web, fino a 1.500 WCU e fino alla dimensione corporea predefinita.

L'attivazione della mitigazione automatica degli attacchi DDoS a livello di applicazione Shield Advanced aggiunge un gruppo di regole all'ACL Web che utilizza 150 unità di capacità ACL Web (WCU). Queste WCU influiscono sull'utilizzo della WCU nell'ACL web. Per ulteriori informazioni, consulta Mitigazione DDoS automatica a livello di applicazione Shield Advanced, Il gruppo di regole Shield Advanced e AWS WAF unità di capacità Web ACL (WCU).

L'abbonamento a Shield Advanced non copre l'uso AWS WAF di risorse che non proteggi utilizzando Shield Advanced. Inoltre, non copre eventuali AWS WAF costi aggiuntivi non standard per le risorse protette. Esempi di AWS WAF costi non standard sono quelli per Bot Control, per l'azione delle CAPTCHA regole, per gli ACL Web che utilizzano più di 1.500 WCU e per l'ispezione del corpo della richiesta oltre le dimensioni corporee predefinite. L'elenco completo è disponibile nella pagina dei prezzi. AWS WAF

Per informazioni complete ed esempi di prezzi, consulta la pagina Prezzi e AWS WAF prezzi di Shield.

Fatturazione dell'abbonamento Shield Advanced

Se sei un AWS Channel Reseller, contatta il team del tuo account per informazioni e assistenza. Queste informazioni di fatturazione sono destinate ai clienti che non sono rivenditori di AWS canale.

Per tutti gli altri, si applicano le seguenti linee guida per l'abbonamento e la fatturazione:

- Per gli account membri di un' AWS Organizations organizzazione, AWS addebita gli abbonamenti Shield Advanced sul conto pagante dell'organizzazione, indipendentemente dal fatto che l'account di pagamento stesso sia sottoscritto.
- Quando sottoscrivi più account appartenenti alla stessa famiglia di conti di fatturazione AWS Organizations consolidati, un unico prezzo di abbonamento copre tutti gli account sottoscritti della famiglia. L'organizzazione deve possedere tutte Account AWS e tutte le proprie risorse.
- Quando sottoscrivi più account per più organizzazioni, puoi comunque pagare un'unica quota di abbonamento per tutte le organizzazioni, gli account e le risorse, purché tu ne sia il proprietario.

Contatta il tuo account manager o l' AWS assistenza e richiedi un'esenzione dai costi di AWS Shield Advanced abbonamento per tutte le organizzazioni tranne una.

Per informazioni dettagliate ed esempi sui prezzi, consulta AWS Shield Prezzi.

Identificazione delle applicazioni da proteggere

Prendi in considerazione l'implementazione delle protezioni Shield Advanced per le applicazioni in cui è necessario uno dei seguenti elementi:

- Disponibilità garantita per gli utenti dell'applicazione.
- Accesso rapido agli esperti di mitigazione DDoS se l'applicazione è interessata da un attacco DDoS.
- Consapevolezza del AWS fatto che l'applicazione potrebbe essere interessata da un attacco DDoS e notifica degli attacchi da parte dei team AWS addetti alla sicurezza o alle operazioni.
- La prevedibilità dei costi del cloud, anche quando un attacco DDoS influisce sull'utilizzo dei servizi. AWS

Se un'applicazione o le relative risorse richiedono una delle opzioni precedenti, valuta la possibilità di creare abbonamenti per i relativi account.

Identificazione delle risorse da proteggere

Per ogni account sottoscritto, valuta la possibilità di aggiungere una protezione Shield Advanced a ciascuna risorsa che presenta una delle seguenti caratteristiche:

- La risorsa serve utenti esterni su Internet.
- La risorsa è esposta a Internet e fa anche parte di un'applicazione critica. Considerate ogni risorsa esposta, indipendentemente dal fatto che intendiate che sia accessibile agli utenti su Internet.
- La risorsa è protetta da un ACL AWS WAF web.

Per ulteriori informazioni sulla creazione e la gestione delle protezioni per le risorse, consulta. Protezione delle risorse in AWS Shield Advanced

Inoltre, segui i consigli di questa guida per assicurarti di progettare la tua applicazione per la resilienza DDoS e di aver configurato correttamente le funzionalità di Shield Advanced per una protezione ottimale.

Esempi di attacchi DDoS

AWS Shield Advanced offre una protezione estesa contro molti tipi di attacchi.

L'elenco seguente descrive alcuni tipi di attacco comuni:

Attacchi di reflection UDP (User Datagram Protocol, Protocollo datagramma utente)

Negli attacchi di riflessione UDP, un utente malintenzionato può falsificare l'origine di una richiesta e utilizzare UDP per ottenere una risposta ampia dal server. Il traffico di rete aggiuntivo diretto verso l'indirizzo IP contraffatto e attaccato può rallentare il server preso di mira e impedire agli utenti finali legittimi di accedere alle risorse necessarie.

Inondazione TCP SYN

L'intento di un attacco TCP SYN flood è quello di esaurire le risorse disponibili di un sistema lasciando le connessioni in uno stato semiaperto. Quando un utente si connette a un servizio TCP come un server web, il client invia un pacchetto TCP SYN. Il server restituisce il suo campo di conferma e il client restituisce il proprio, completando l'handshake a tre. In un flusso TCP SYN, il terzo riconoscimento non viene mai restituito e il server rimane in attesa di una risposta. Questo può impedire ad altri utenti di connettersi al server.

Flood di query DNS

In un flusso di query DNS, un utente malintenzionato utilizza più query DNS per esaurire le risorse di un server DNS. AWS Shield Advanced può contribuire a fornire protezione contro gli attacchi di query DNS flood sui server DNS Route 53.

Attacchi flood HTTP o rottura della cache (livello 7)

Con un HTTP flood, che include `GET` and `POST` floods, un utente malintenzionato invia più richieste HTTP che sembrano provenire da un utente reale dell'applicazione web. Gli attacchi di rottura della cache sono un tipo di flood HTTP che utilizzano variazioni nella stringa di query di richieste HTTP che impediscono l'utilizzo di contenuti memorizzati nella cache edge located. Questo tipo di attacchi forzano l'esecuzione dei contenuti dal server Web di origine, causando deformazioni ulteriori e potenzialmente dannose al server Web di origine.

Come AWS Shield rileva gli eventi

AWS utilizza sistemi di rilevamento a livello di servizio per la AWS rete e AWS i singoli servizi, per garantire che rimangano disponibili durante un attacco DDoS. Inoltre, i sistemi di rilevamento a livello

di risorsa monitorano ogni singola AWS risorsa per garantire che il traffico verso la risorsa rimanga entro i parametri previsti. Questa combinazione protegge sia la AWS risorsa che i AWS servizi interessati, applicando misure di mitigazione che eliminano i pacchetti noti non validi, evidenziano il traffico potenzialmente dannoso e danno priorità al traffico proveniente dagli utenti finali.

Gli eventi rilevati vengono visualizzati nei riepiloghi degli eventi di Shield Advanced, nei dettagli degli attacchi e nelle CloudWatch metriche di Amazon come nome del vettore di attacco DDoS o come `Volumetric` se la valutazione fosse basata sul volume di traffico anziché sulla firma. Per ulteriori informazioni sulle dimensioni del vettore di attacco disponibili all'interno della metrica, consulta `DDoSDetected` CloudWatch AWS Shield Advanced metriche

Argomenti

- Logica di rilevamento delle minacce a livello di infrastruttura
- Logica di rilevamento per le minacce a livello di applicazione
- Logica di rilevamento per più risorse in un'applicazione

Logica di rilevamento delle minacce a livello di infrastruttura

La logica di rilevamento utilizzata per proteggere AWS le risorse mirate dagli attacchi DDoS nei livelli dell'infrastruttura (livello 3 e livello 4) dipende dal tipo di risorsa e dal fatto che la risorsa sia protetta o meno. AWS Shield Advanced

Rilevamento per Amazon CloudFront e Amazon Route 53

Quando servi un'applicazione Web con CloudFront e Route 53, tutti i pacchetti dell'applicazione vengono ispezionati da un sistema di mitigazione DDoS completamente in linea, che non introduce alcuna latenza osservabile. Gli attacchi DDoS contro le CloudFront distribuzioni e le zone ospitate da Route 53 vengono mitigati in tempo reale. Queste protezioni si applicano indipendentemente dal fatto che si utilizzi. AWS Shield Advanced

Segui la best practice di utilizzare CloudFront Route 53 come punto di ingresso della tua applicazione web, ove possibile, per il rilevamento e la mitigazione più rapidi degli eventi DDoS.

Rilevamento AWS Global Accelerator e servizi regionali

Il rilevamento a livello di risorsa protegge gli acceleratori e le risorse AWS Global Accelerator standard lanciati nelle AWS regioni, come Classic Load Balancer, Application Load Balancer e Elastic IP address (EIP). Questi tipi di risorse vengono monitorati per rilevare aumenti del traffico che possono indicare la presenza di un attacco DDoS che richiede una mitigazione. Ogni minuto, viene

valutato il traffico verso ogni AWS risorsa. Se il traffico verso una risorsa è elevato, vengono eseguiti controlli aggiuntivi per misurare la capacità della risorsa.

Shield esegue i seguenti controlli standard:

- Istanze Amazon Elastic Compute Cloud (Amazon EC2), EIP collegati a istanze Amazon EC2: Shield recupera la capacità dalla risorsa protetta. La capacità dipende dal tipo di istanza della destinazione, dalla dimensione dell'istanza e da altri fattori, ad esempio se l'istanza utilizza una rete avanzata.
- Classic Load Balancer e Application Load Balancer: Shield recupera la capacità dal nodo di bilanciamento del carico di destinazione.
- EIP collegati a Network Load Balancers — Shield recupera la capacità dal load balancer di destinazione. La capacità è indipendente dalla configurazione di gruppo del sistema di bilanciamento del carico di destinazione.
- AWS Global Accelerator acceleratori standard: Shield recupera la capacità, che si basa sulla configurazione dell'endpoint.

Queste valutazioni si verificano su più dimensioni del traffico di rete, come porta e protocollo. Se viene superata la capacità della risorsa di destinazione, Shield effettua una mitigazione degli attacchi DDoS. Le mitigazioni introdotte da Shield ridurranno il traffico DDoS, ma potrebbero non eliminarlo. Shield può inoltre porre rimedio se viene superata una frazione della capacità della risorsa su una dimensione di traffico coerente con i vettori di attacco DDoS noti. Shield colloca questa mitigazione con un tempo di vita limitato (TTL), che estende finché l'attacco è in corso.

> **Note**
>
> Le mitigazioni applicate da Shield ridurranno il traffico DDoS, ma potrebbero non eliminarlo. Puoi potenziare Shield con soluzioni come AWS Network Firewall o un firewall on-host iptables per impedire all'applicazione di elaborare traffico non valido per l'applicazione o non generato da utenti finali legittimi.

Le protezioni Shield Advanced aggiungono quanto segue alle attività di rilevamento Shield esistenti:

- Soglie di rilevamento inferiori: Shield Advanced colloca le mitigazioni alla metà della capacità calcolata. Ciò può fornire mitigazioni più rapide per gli attacchi che aumentano lentamente e mitigare gli attacchi che hanno una firma volumetrica più ambigua.

- Protezione dagli attacchi intermittenti: Shield Advanced implementa le mitigazioni con un time to live (TTL) che aumenta esponenzialmente, in base alla frequenza e alla durata degli attacchi. In questo modo le mitigazioni rimangono attive più a lungo quando una risorsa viene spesso presa di mira e quando un attacco si verifica a raffiche brevi.
- Rilevamento basato sullo stato: quando si associa un controllo dello stato di Route 53 a una risorsa protetta Shield Advanced, lo stato del controllo dello stato viene utilizzato nella logica di rilevamento. Durante un evento rilevato, se il controllo dello stato di salute è corretto, Shield Advanced richiede una maggiore sicurezza che si tratti di un attacco prima di effettuare una mitigazione. Se invece il controllo sanitario non è salutare, Shield Advanced potrebbe porre una mitigazione ancor prima che sia stata stabilita la fiducia. Questa funzionalità aiuta a evitare i falsi positivi e fornisce reazioni più rapide agli attacchi che colpiscono l'applicazione. Per informazioni sui controlli sanitari con Shield Advanced, vedereRilevamento basato sulla salute mediante controlli sanitari.

Logica di rilevamento per le minacce a livello di applicazione

AWS Shield Advanced fornisce il rilevamento a livello di applicazione Web per CloudFront distribuzioni Amazon protette e Application Load Balancer. Quando proteggi questi tipi di risorse con Shield Advanced, puoi associare un ACL AWS WAF Web alla tua protezione per abilitare il rilevamento a livello di applicazione Web. Shield Advanced utilizza i dati di richiesta per l'ACL Web associato e crea una linea di base del traffico per l'applicazione. Il rilevamento del livello di applicazione Web si basa sull'integrazione nativa tra Shield Advanced e AWS WAF. Per ulteriori informazioni sulle protezioni a livello di applicazione, inclusa l'associazione di un ACL AWS WAF Web a una risorsa protetta Shield Advanced, consulta. AWS Shield Advanced protezioni a livello di applicazione (livello 7)

Per il rilevamento a livello di applicazione Web, Shield Advanced monitora il traffico delle applicazioni e lo confronta con le linee di base storiche alla ricerca di anomalie. Questo monitoraggio copre il volume totale e la composizione del traffico. Durante un attacco DDoS, ci aspettiamo che il volume e la composizione del traffico cambino e Shield Advanced richiede una deviazione statisticamente significativa in entrambi i casi per dichiarare un evento.

Shield Advanced esegue le sue misurazioni rispetto alle finestre temporali storiche. Questo approccio riduce le notifiche di falsi positivi derivanti da variazioni legittime del volume di traffico o da variazioni del traffico che corrispondono a uno schema previsto, ad esempio una vendita offerta ogni giorno alla stessa ora.

> **Note**
>
> Evita i falsi positivi nelle tue protezioni Shield Advanced concedendo a Shield Advanced il tempo di stabilire linee di base che rappresentino modelli di traffico normali e legittimi. Shield Advanced inizia a raccogliere informazioni per la sua linea di base quando si associa un ACL Web alla risorsa protetta. Associate un ACL Web alla risorsa protetta almeno 24 ore prima di qualsiasi evento pianificato che potrebbe causare schemi insoliti nel traffico web. Il rilevamento del livello di applicazione Web Shield Advanced è più preciso quando ha osservato 30 giorni di traffico normale.

Il tempo impiegato da Shield Advanced per rilevare un evento è influenzato dalla variazione osservata nel volume di traffico. Per variazioni di volume inferiori, Shield Advanced osserva il traffico per un periodo più lungo, al fine di aumentare la sicurezza che si stia verificando un evento. Per variazioni di volume più elevate, Shield Advanced rileva e segnala un evento più rapidamente.

Una regola basata sulla frequenza nell'ACL Web, aggiunta da te o dalla funzionalità di mitigazione automatica del livello di applicazione Shield Advanced, può mitigare un attacco prima che raggiunga un livello rilevabile. Per ulteriori informazioni sulla mitigazione automatica degli attacchi DDoS a livello di applicazione, consulta. Mitigazione DDoS automatica a livello di applicazione Shield Advanced

> **Note**
>
> È possibile progettare l'applicazione in modo che sia scalabile in risposta a traffico o carico elevati per garantire che non sia influenzata da flussi di richieste di minore entità. Con Shield Advanced, le risorse protette sono coperte dalla protezione dei costi. Questo ti aiuta a proteggerti da aumenti imprevisti della bolletta del cloud che potrebbero verificarsi a seguito di un attacco DDoS. Per ulteriori informazioni sulla protezione dei costi Shield Advanced, consultaRichiedere un credito in AWS Shield Advanced.

Logica di rilevamento per più risorse in un'applicazione

È possibile utilizzare i gruppi di AWS Shield Advanced protezione per creare raccolte di risorse protette che fanno parte della stessa applicazione. È possibile scegliere quali risorse protette inserire in un gruppo o indicare che tutte le risorse dello stesso tipo devono essere trattate come un unico gruppo. Ad esempio, è possibile creare un gruppo di tutti gli Application Load Balancer. Quando si crea un gruppo di protezione, il rilevamento Shield Advanced aggrega tutto il traffico per le risorse

protette all'interno del gruppo. Ciò è utile se si dispone di molte risorse, ognuna con una piccola quantità di traffico, ma con un grande volume aggregato. È inoltre possibile utilizzare i gruppi di protezione per preservare le linee di base delle applicazioni, nel caso di implementazioni blu-verdi in cui il traffico viene trasferito tra risorse protette.

Puoi scegliere di aggregare il traffico nel tuo gruppo di protezione in uno dei seguenti modi:

- Somma: questa aggregazione combina tutto il traffico tra le risorse del gruppo di protezione. È possibile utilizzare questa aggregazione per garantire che le nuove risorse create abbiano una base di riferimento esistente e per ridurre la sensibilità al rilevamento, il che può aiutare a prevenire i falsi positivi.
- Media: questa aggregazione utilizza la media di tutto il traffico all'interno del gruppo di protezione. È possibile utilizzare questa aggregazione per applicazioni in cui il traffico tra le risorse è uniforme, come i sistemi di bilanciamento del carico.
- Max: questa aggregazione utilizza il traffico più elevato di qualsiasi risorsa del gruppo di protezione. È possibile utilizzare questa aggregazione quando vi sono più livelli di un'applicazione in un gruppo di protezione. Ad esempio, potresti avere un gruppo di protezione che include una CloudFront distribuzione, la relativa origine Application Load Balancer e gli obiettivi dell'istanza Amazon EC2 di Application Load Balancer.

Puoi anche utilizzare i gruppi di protezione per migliorare la velocità con cui Shield Advanced effettua le mitigazioni, per gli attacchi che prendono di mira più IP elastici o acceleratori standard connessi a Internet. AWS Global Accelerator Quando viene presa di mira una risorsa in un gruppo di protezione, Shield Advanced stabilisce la fiducia per le altre risorse del gruppo. Ciò mette in allerta il rilevamento Shield Advanced e può ridurre il tempo necessario per creare ulteriori mitigazioni.

Per ulteriori informazioni sui gruppi di protezione, consultaAWS Shield Advanced gruppi di protezione.

Come AWS Shield mitigare gli eventi

La logica di mitigazione che protegge l'applicazione può variare a seconda dell'architettura dell'applicazione. Quando proteggi un'applicazione Web con Amazon CloudFront e Amazon Route 53, usufruisci di mitigazioni specifiche per i casi d'uso Web e DNS e che proteggono tutto il traffico per i servizi. Quando il punto di ingresso dell'applicazione è una risorsa che viene eseguita in una AWS regione, la logica di mitigazione varia a seconda del servizio, del tipo di risorsa e dell'utilizzo che ne fai. AWS Shield Advanced

AWS I sistemi di mitigazione degli attacchi DDoS sono sviluppati dagli ingegneri di Shield e sono strettamente integrati con AWS i servizi. Gli ingegneri tengono conto di aspetti dell'architettura, come la capacità e lo stato delle risorse mirate. Gli ingegneri di Shield monitorano continuamente l'efficacia e le prestazioni dei sistemi di mitigazione degli attacchi DDoS e sono in grado di rispondere rapidamente quando vengono scoperte o previste nuove minacce.

Puoi progettare la tua applicazione in modo che sia scalabile in risposta a traffico o carico elevati, per garantire che non sia influenzata da minori ondate di richieste. Se utilizzi Shield Advanced per proteggere le tue risorse, ricevi una copertura contro gli aumenti imprevisti della bolletta del cloud che potrebbero verificarsi a seguito di un attacco DDoS.

Mitigazioni dell'infrastruttura

Per gli attacchi a livello di infrastruttura, i sistemi di mitigazione AWS Shield DDoS sono presenti ai confini della AWS rete e nelle posizioni periferiche. AWS Il posizionamento di più livelli di controlli di sicurezza in tutta l' AWS infrastruttura consente di gestire defense-in-depth le applicazioni cloud.

Shield mantiene i sistemi di mitigazione degli attacchi DDoS in tutti i punti di ingresso da Internet. Quando Shield rileva un attacco DDoS, per ogni punto di ingresso, reindirizza il traffico attraverso i sistemi di mitigazione DDoS nella stessa posizione. Ciò non introduce alcuna latenza aggiuntiva osservabile e fornisce una capacità di mitigazione di oltre 100 TeraBits al secondo (Tbps) in tutte le regioni e tutte le edge location. AWS Shield protegge la disponibilità delle risorse senza reindirizzare il traffico verso centri di lavaggio esterni o remoti, il che potrebbe aumentare la latenza.

- Ai confini della AWS rete, per qualsiasi AWS servizio o risorsa, i sistemi di mitigazione DDoS mitigano gli attacchi a livello di infrastruttura provenienti da Internet. I sistemi eseguono le loro mitigazioni quando segnalati dal rilevamento Shield o da un tecnico dello Shield Response Team (SRT).
- Nelle sedi AWS periferiche, i sistemi di mitigazione degli attacchi DDoS ispezionano continuamente ogni pacchetto inoltrato alle distribuzioni Amazon CloudFront e alle zone ospitate di Amazon Route 53, indipendentemente dalla loro origine. Quando necessario, i sistemi applicano mitigazioni progettate specificamente per il traffico web e DNS. Un ulteriore vantaggio dell'utilizzo di Amazon CloudFront e Amazon Route 53 per proteggere le applicazioni Web è che gli attacchi DDoS vengono immediatamente mitigati, senza richiedere un segnale proveniente dal rilevamento Shield.

Mitigazioni a livello di applicazione

Shield Advanced fornisce mitigazioni a livello di applicazione Web per le CloudFront distribuzioni Amazon e gli Application Load Balancer in cui hai abilitato le protezioni Shield Advanced. Quando

abiliti la protezione, associ un ACL AWS WAF web alla risorsa, per abilitare il rilevamento a livello di applicazione web. Inoltre, hai la possibilità di abilitare la mitigazione automatica a livello di applicazione, che indica a Shield Advanced di gestire le protezioni per te durante un attacco DDoS.

Shield fornisce solo mitigazioni personalizzate per gli attacchi a livello di applicazione alle risorse per le quali hai abilitato Shield Advanced e la mitigazione automatica a livello di applicazione. Con la mitigazione automatica, Shield Advanced impone la limitazione della AWS WAF velocità sulle richieste provenienti da fonti DDoS note e aggiunge e gestisce automaticamente AWS WAF protezioni personalizzate in risposta agli attacchi DDoS rilevati. Per informazioni dettagliate sulle mitigazioni di questo tipo, vedere. Come Shield Advanced gestisce la mitigazione automatica

Una regola basata sulla frequenza nell'ACL Web, aggiunta da te o aggiunta dalla funzionalità di mitigazione automatica del livello di applicazione Shield Advanced, può mitigare un attacco prima che raggiunga un livello rilevabile. Per ulteriori informazioni sul rilevamento, vedere. Logica di rilevamento per le minacce a livello di applicazione

Funzionalità di mitigazione

Le caratteristiche principali della mitigazione degli AWS Shield attacchi DDoS sono le seguenti:

- Convalida dei pacchetti: garantisce che ogni pacchetto ispezionato sia conforme a una struttura prevista e sia valido per il relativo protocollo. Le convalide dei protocolli supportate includono IP, TCP (inclusi header e opzioni), UDP, ICMP, DNS e NTP.
- Liste di controllo degli accessi (ACL) e shaper: un ACL valuta il traffico in base a attributi specifici e elimina il traffico corrispondente o lo mappa su uno shaper. Lo shaper limita la frequenza dei pacchetti per il traffico corrispondente, eliminando i pacchetti in eccesso per contenere il volume che raggiunge la destinazione. AWS Shield i tecnici del detection e dello Shield Response Team (SRT) possono fornire allocazioni di tariffe dedicate al traffico previsto e allocazioni di tariffe più restrittive al traffico con attributi che corrispondono ai vettori di attacco DDoS noti. Gli attributi che un ACL può corrispondere includono la porta, il protocollo, i flag TCP, l'indirizzo di destinazione, il paese di origine e gli schemi arbitrari nel payload del pacchetto.
- Punteggio sospetto: utilizza la conoscenza che Shield ha del traffico previsto per applicare un punteggio a ogni pacchetto. Ai pacchetti che aderiscono maggiormente ai modelli di traffico noto come buono viene assegnato un punteggio di sospetto più basso. L'osservazione di attributi noti di traffico non valido può aumentare il punteggio di sospetto per un pacchetto. Quando è necessario stabilire un limite di velocità per i pacchetti, Shield rilascia per primi i pacchetti con punteggi di sospetto più alti. Questo aiuta Shield a mitigare gli attacchi DDoS noti e zero-day evitando al contempo i falsi positivi.

- Proxy TCP SYN: fornisce protezione contro i flood TCP SYN inviando cookie TCP SYN per contestare nuove connessioni prima di consentirne il passaggio al servizio protetto. Il proxy TCP SYN fornito da Shield DDoS mitigation è stateless, il che gli consente di mitigare i più grandi attacchi TCP SYN flood conosciuti senza raggiungere l'esaurimento dello stato. Ciò si ottiene integrando i AWS servizi per trasferire lo stato della connessione invece di mantenere un proxy continuo tra il client e il servizio protetto. Il proxy TCP SYN è attualmente disponibile su Amazon e CloudFront Amazon Route 53.
- Distribuzione delle tariffe: regola continuamente i valori dello shaper per località in base al modello di ingresso del traffico verso una risorsa protetta. Ciò impedisce la limitazione della velocità del traffico dei clienti che potrebbe non entrare nella rete in modo uniforme. AWS

AWS Shield logica di mitigazione per CloudFront e Route 53

La mitigazione degli attacchi DDoS di Shield ispeziona continuamente il traffico e la Route 53 CloudFront . Questi servizi operano da una rete di AWS edge location distribuita a livello globale che offre un ampio accesso alla capacità di mitigazione degli attacchi DDoS di Shield e distribuisce l'applicazione da un'infrastruttura più vicina agli utenti finali.

- CloudFront— Le mitigazioni DDoS Shield consentono solo al traffico valido per le applicazioni Web di passare al servizio. Ciò fornisce una protezione automatica contro molti vettori DDoS comuni, come gli attacchi di riflessione UDP.

  CloudFront mantiene connessioni persistenti all'origine dell'applicazione, i flood TCP SYN vengono automaticamente mitigati attraverso l'integrazione con la funzione proxy Shield TCP SYN e Transport Layer Security (TLS) viene terminato all'edge. Queste funzionalità combinate assicurano che l'origine dell'applicazione riceva solo richieste Web ben formate e che sia protetta da attacchi DDoS di livello inferiore, flood di connessione e abuso di TLS.

  CloudFront utilizza una combinazione di direzione del traffico DNS e routing anycast. Queste tecniche migliorano la resilienza dell'applicazione mitigando gli attacchi vicini alla fonte, fornendo l'isolamento dai guasti e garantendo l'accesso alla capacità di mitigare gli attacchi più grandi conosciuti.
- Le mitigazioni Route 53 — Shield consentono solo a richieste DNS valide di raggiungere il servizio. Shield mitiga i flussi di query DNS utilizzando un sistema di punteggio di sospetto che dà priorità alle query note con esito positivo e riduce la priorità alle query che contengono attributi di attacco DDoS sospetti o noti.

Route 53 utilizza lo shuffle sharding per fornire un set unico di quattro indirizzi IP resolver per ogni zona ospitata, sia per IPv4 che per IPv6. Ogni indirizzo IP corrisponde a un sottoinsieme diverso di posizioni Route 53. Ogni sottoinsieme di posizioni è costituito da server DNS autorevoli che si sovrappongono solo parzialmente all'infrastruttura di qualsiasi altro sottoinsieme. In questo modo, se una richiesta dell'utente non riesce per qualsiasi motivo, verrà inviata correttamente in caso di nuovo tentativo.

Route 53 utilizza il routing anycast per indirizzare le query DNS alla edge location più vicina, in base alla prossimità della rete. Anycast invia inoltre il traffico DDoS verso molte edge location, impedendo agli attacchi di concentrarsi su un'unica posizione.

Oltre alla velocità di mitigazione, CloudFront Route 53 offre un ampio accesso alla capacità distribuita a livello globale di Shield. Per sfruttare queste funzionalità, utilizzate questi servizi come punto di ingresso per le vostre applicazioni web dinamiche o statiche.

Per ulteriori informazioni sull'utilizzo CloudFront di Route 53 per proteggere le applicazioni Web, consulta Come proteggere le applicazioni Web dinamiche dagli attacchi DDoS utilizzando Amazon CloudFront e Amazon Route 53. Per ulteriori informazioni sull'isolamento dei guasti su Route 53, consulta A Case Study in Global Fault Isolation.

AWS Shield logica di mitigazione per le regioni AWS

Le risorse lanciate nelle AWS Regioni sono protette da sistemi di mitigazione AWS Shield DDoS posizionati dal rilevamento a livello di risorsa Shield. Le risorse regionali includono Elastic IP (EIP), Classic Load Balancers e Application Load Balancers.

Prima di effettuare una mitigazione, Shield identifica la risorsa bersaglio e la sua capacità. Shield utilizza la capacità di determinare il traffico totale massimo che le sue mitigazioni dovrebbero consentire di inoltrare alla risorsa. Le liste di controllo degli accessi (ACL) e altri shaper inclusi nella mitigazione potrebbero ridurre i volumi consentiti per parte del traffico, ad esempio il traffico che corrisponde ai vettori di attacco DDoS noti o che non dovrebbe avere un volume elevato. Ciò limita ulteriormente la quantità di traffico consentita dalle mitigazioni per gli attacchi di riflessione UDP o per il traffico TCP con flag TCP SYN o FIN.

Shield determina la capacità e posiziona le mitigazioni in modo diverso per ogni tipo di risorsa.

- Per un'istanza Amazon EC2 o un EIP collegato a un'istanza Amazon EC2, Shield calcola la capacità in base al tipo di istanza e ad altri attributi dell'istanza, ad esempio se l'istanza ha una rete avanzata abilitata.
- Per un Application Load Balancer o un Classic Load Balancer, Shield calcola la capacità individualmente per ogni nodo di destinazione del load balancer. Le mitigazioni degli attacchi DDoS per queste risorse sono fornite da una combinazione di mitigazioni DDoS Shield e scalabilità automatica da parte del load balancer. Quando lo Shield Response Team (SRT) è impegnato in un attacco contro una risorsa Application Load Balancer o Classic Load Balancer, potrebbe accelerare la scalabilità come misura di protezione aggiuntiva.
- Shield calcola che la capacità di alcune AWS risorse si basa sulla capacità disponibile dell' AWS infrastruttura sottostante. Questi tipi di risorse includono Network Load Balancer (NLB) e risorse che instradano il traffico attraverso Gateway Load Balancers o. AWS Network Firewall

> **Note**
>
> Proteggi i tuoi Network Load Balancer collegando EIP protetti da Shield Advanced. Puoi lavorare con SRT per creare mitigazioni personalizzate basate sul traffico e sulla capacità previsti dell'applicazione sottostante.

Quando Shield effettua una mitigazione, i limiti di velocità iniziali definiti da Shield nella logica di mitigazione vengono applicati allo stesso modo a tutti i sistemi di mitigazione DDoS Shield. Ad esempio, se Shield applica una mitigazione con un limite di 100.000 pacchetti al secondo (pps), inizialmente consentirà 100.000 pps in ogni posizione. Quindi, Shield aggrega continuamente le metriche di mitigazione per determinare il rapporto effettivo del traffico e utilizza il rapporto per adattare il limite di velocità per ciascuna località. Ciò previene i falsi positivi e garantisce che le mitigazioni non siano eccessivamente permissive.

AWS Shield logica di mitigazione per acceleratori AWS Global Accelerator standard

Le mitigazioni Shield consentono solo al traffico valido di raggiungere gli endpoint listener di un acceleratore standard Global Accelerator. Gli acceleratori standard sono distribuiti a livello globale e forniscono indirizzi IP che è possibile utilizzare per indirizzare il traffico verso risorse in qualsiasi regione. AWS AWS I limiti di velocità che Shield impone per la mitigazione di Global Accelerator si basano sulle capacità delle risorse verso le quali l'acceleratore standard indirizza il traffico. Shield applica misure di mitigazione quando il traffico totale supera la velocità determinata e anche quando viene superata una frazione di tale velocità per i vettori DDoS noti.

Quando configuri un acceleratore standard, definisci i gruppi di endpoint per ogni AWS regione in cui indirizzerai il traffico per la tua applicazione. Quando Shield effettua una mitigazione, calcola la capacità di ciascun gruppo di endpoint e aggiorna di conseguenza i limiti di velocità in ogni sistema di mitigazione DDoS Shield. La tariffa varia per ogni località, in base alle ipotesi formulate da Shield sul modo in cui il traffico verrà indirizzato da Internet alle tue AWS risorse. La capacità di un gruppo di endpoint viene calcolata come il numero di risorse del gruppo moltiplicato per la capacità più bassa di qualsiasi risorsa del gruppo. A intervalli regolari, Shield ricalcola la capacità dell'applicazione e aggiorna i limiti di velocità secondo necessità.

> **Note**
>
> L'utilizzo delle ghiere di traffico per modificare la percentuale di traffico indirizzato a un gruppo di endpoint non modifica il modo in cui Shield calcola o distribuisce i limiti di velocità nei suoi sistemi di mitigazione degli attacchi DDoS. Se utilizzi le chiamate di traffico, configura i gruppi di endpoint in modo che si rispecchino a vicenda in termini di tipo e quantità di risorse. Questo aiuta a garantire che la capacità calcolata da Shield sia rappresentativa delle risorse che servono il traffico dell'applicazione.

Per ulteriori informazioni sui gruppi di endpoint e sui quadranti di traffico in Global Accelerator, consulta Gruppi di endpoint negli acceleratori standard. AWS Global Accelerator

AWS Shield Advanced logica di mitigazione per IP elastici

Quando proteggi un IP elastico (EIP) con AWS Shield Advanced, Shield Advanced migliora le mitigazioni applicate da Shield durante un evento DDoS. I sistemi di mitigazione DDoS Shield Advanced replicano la configurazione Network ACL (NACL) per la sottorete pubblica a cui è associata l'EIP. Ad esempio, se il tuo NACL è configurato per bloccare tutto il traffico UDP, Shield Advanced unisce tale regola alle mitigazioni applicate da Shield.

Questa funzionalità aggiuntiva può aiutarti a evitare i rischi di disponibilità dovuti al traffico non valido per la tua applicazione. È inoltre possibile utilizzare i NAC per bloccare singoli indirizzi IP di origine o intervalli CIDR di indirizzi IP di origine. Questo può essere un utile strumento di mitigazione per gli attacchi DDoS che non sono distribuiti. Inoltre, consente di gestire facilmente elenchi di indirizzi consentiti o di bloccare gli indirizzi IP che non dovrebbero comunicare con l'applicazione, senza fare affidamento sull'intervento dei tecnici. AWS

AWS Shield Advanced logica di mitigazione per applicazioni web

AWS Shield Advanced utilizza AWS WAF per mitigare gli attacchi a livello di applicazioni Web. AWS WAF è incluso in Shield Advanced senza costi aggiuntivi.

Protezione standard a livello di applicazione

Quando proteggi una CloudFront distribuzione Amazon o Application Load Balancer con Shield Advanced, puoi utilizzare Shield Advanced per associare un ACL AWS WAF web alla tua risorsa protetta, se non ne hai già uno associato. Se non hai già configurato un ACL Web, puoi utilizzare la procedura guidata della console Shield Advanced per crearne uno e aggiungervi una regola basata sulla frequenza. Una regola basata sulla frequenza limita il numero di richieste per ogni finestra temporale di cinque minuti per ogni indirizzo IP, fornendo protezioni di base contro i flussi di richieste a livello di applicazione Web. È possibile configurare la tariffa, a partire da un minimo di 100. Per ulteriori informazioni, consulta ACL AWS WAF Web Shield Advanced a livello applicativo e regole basate sulla velocità.

Puoi anche utilizzare il AWS WAF servizio per gestire l'ACL web. Tramite AWS WAF, puoi espandere la configurazione Web ACL per eseguire operazioni come ispezionare componenti specifici della richiesta Web per verificare corrispondenze o modelli di stringhe, aggiungere una gestione personalizzata di richieste e risposte e confrontare la geolocalizzazione dell'origine della richiesta. Per ulteriori informazioni sulle AWS WAF regole, consulta. AWS WAF regole

Mitigazione automatica a livello di applicazione

Per una protezione avanzata, abilita la mitigazione automatica del livello di applicazione Shield Advanced. Con questa opzione, Shield Advanced mantiene una regola AWS WAF di limitazione della velocità per le richieste provenienti da fonti DDoS note e fornisce mitigazioni personalizzate per gli attacchi DDoS rilevati.

Quando Shield Advanced rileva un attacco a una risorsa protetta, tenta di identificare una firma di attacco che isola il traffico di attacco dal normale traffico verso l'applicazione. Shield Advanced valuta la firma dell'attacco identificata rispetto ai modelli di traffico storici per la risorsa sotto attacco, nonché per qualsiasi altra risorsa associata allo stesso ACL web.

Se Shield Advanced determina che la firma di attacco isola solo il traffico coinvolto nell'attacco DDoS, implementa la firma nelle AWS WAF regole all'interno dell'ACL web associato. Puoi indicare a Shield Advanced di implementare mitigazioni che contino solo il traffico a cui corrispondono o che lo blocchino, e puoi modificare l'impostazione in qualsiasi momento. Quando Shield Advanced

determina che le sue regole di mitigazione non sono più necessarie, le rimuove dall'ACL Web. Per ulteriori informazioni sulla mitigazione degli eventi a livello di applicazione, vedere. Mitigazione DDoS automatica a livello di applicazione Shield Advanced

Per ulteriori informazioni sulle mitigazioni a livello di applicazione Shield Advanced, vedereAWS Shield Advanced protezioni a livello di applicazione (livello 7).

Esempi di architetture resilienti agli attacchi DDoS di base

La resilienza DDoS è la capacità dell'architettura applicativa di resistere agli attacchi Distributed Denial of Service (DDoS) continuando a servire utenti finali legittimi. Un'applicazione altamente resiliente può rimanere disponibile durante un attacco con un impatto minimo sui parametri prestazionali come errori o latenza. Questa sezione mostra alcune architetture di esempio comuni e descrive come utilizzare le funzionalità di rilevamento e mitigazione degli attacchi DDoS fornite da AWS Shield Advanced per aumentarne la resilienza agli attacchi DDoS.

Le architetture di esempio in questa sezione evidenziano i AWS servizi che offrono i maggiori vantaggi in termini di resilienza DDoS per le applicazioni distribuite. I vantaggi dei servizi evidenziati includono quanto segue:

- Accesso alla capacità di rete distribuita a livello globale: i servizi Amazon CloudFront e Amazon Route 53 forniscono l'accesso a Internet e alla capacità di mitigazione degli attacchi DDoS attraverso la rete AWS perimetrale globale. AWS Global Accelerator Ciò è utile per mitigare attacchi volumetrici di grandi dimensioni, che possono raggiungere i terabit di scala. È possibile eseguire l'applicazione in qualsiasi AWS regione e utilizzare questi servizi per proteggere la disponibilità e ottimizzare le prestazioni per gli utenti legittimi.
- Protezione dai vettori di attacco DDoS a livello di applicazione Web: gli attacchi DDoS a livello di applicazione Web vengono mitigati al meglio utilizzando una combinazione di scalabilità delle applicazioni e un firewall per applicazioni Web (WAF). Shield Advanced utilizza i registri di ispezione delle richieste Web AWS WAF per rilevare anomalie che possono essere mitigate automaticamente o tramite il coinvolgimento dello AWS Shield Response Team (SRT). La mitigazione automatica è disponibile tramite regole AWS WAF basate sulla frequenza implementate e anche tramite la mitigazione DDoS a livello di applicazione automatica Shield Advanced.

Oltre a esaminare questi esempi, consulta e segui le migliori pratiche applicabili nella sezione Best Practices for DDoS Resiliency.AWS

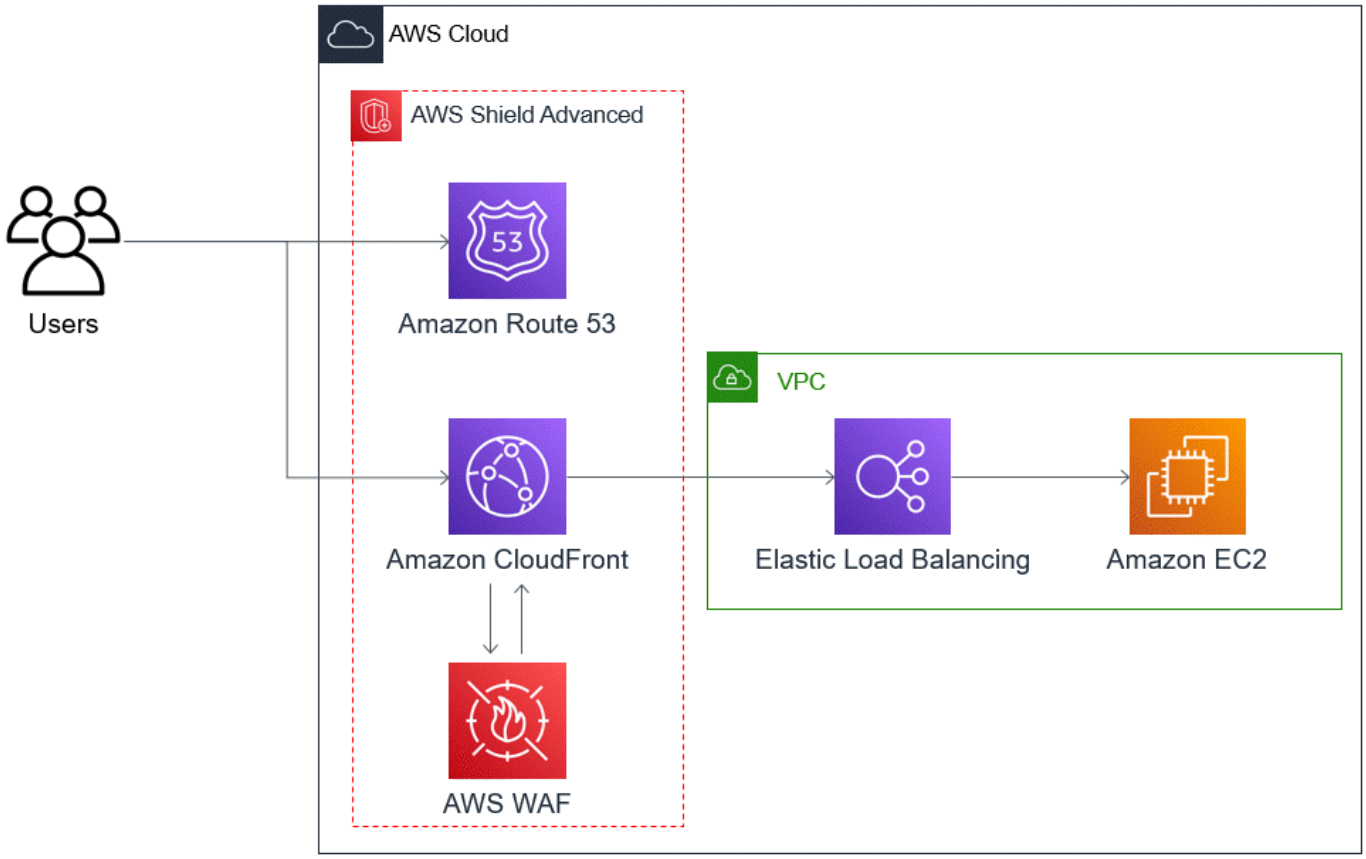
Esempio di resilienza DDoS per applicazioni Web comuni

È possibile creare un'applicazione Web in qualsiasi AWS regione e ricevere una protezione DDoS automatica grazie alle funzionalità di rilevamento e mitigazione disponibili nella regione. AWS

Questo esempio riguarda le architetture che indirizzano gli utenti a un'applicazione Web utilizzando risorse come Classic Load Balancers, Application Load Balancers, Network Load Balancers, soluzioni AWS Marketplace o il proprio livello proxy. Puoi migliorare la resilienza DDoS inserendo zone ospitate Amazon Route 53, distribuzioni CloudFront Amazon AWS WAF e ACL Web tra queste risorse di applicazioni Web e i tuoi utenti. Questi inserimenti possono offuscare l'origine dell'applicazione, servire le richieste più vicino agli utenti finali e rilevare e mitigare i flussi di richieste a livello di applicazione. Le applicazioni che forniscono contenuti statici o dinamici agli utenti con Route 53 sono protette da un sistema di mitigazione DDoS integrato CloudFront e completamente in linea che mitiga gli attacchi a livello di infrastruttura in tempo reale.

Con questi miglioramenti architetturali, puoi quindi proteggere le tue zone ospitate su Route 53 e le tue CloudFront distribuzioni con Shield Advanced. Quando proteggi CloudFront le distribuzioni, Shield Advanced ti richiede di associare gli ACL AWS WAF Web e di creare regole basate sulla frequenza per essi, e ti offre la possibilità di abilitare la mitigazione automatica degli attacchi DDoS a livello di applicazione o il coinvolgimento proattivo. Il coinvolgimento proattivo e la mitigazione automatica degli attacchi DDoS a livello di applicazione utilizzano i controlli di integrità di Route 53 associati alla risorsa. Per ulteriori informazioni su queste opzioni, consulta Protezione delle risorse in AWS Shield Advanced.

Il seguente diagramma di riferimento illustra questa architettura resiliente agli attacchi DDoS per un'applicazione Web.



I vantaggi che questo approccio offre alla tua applicazione web includono i seguenti:

- Protezione dagli attacchi DDoS a livello di infrastruttura utilizzati di frequente (livello 3 e livello 4), senza ritardi di rilevamento. Inoltre, se una risorsa viene spesso presa di mira, Shield Advanced applica misure di mitigazione per periodi di tempo più lunghi. Shield Advanced utilizza anche il contesto dell'applicazione dedotto dagli ACL di rete (NAC) per bloccare il traffico indesiderato più a monte. In questo modo i guasti vengono isolati più vicino alla fonte, riducendo al minimo l'effetto sugli utenti legittimi.
- Protezione contro le inondazioni TCP SYN. I sistemi di mitigazione DDoS integrati con CloudFront Route 53 AWS Global Accelerator forniscono una funzionalità proxy TCP SYN che sfida i nuovi tentativi di connessione e serve solo utenti legittimi.
- Protezione dagli attacchi a livello di applicazione DNS, poiché Route 53 è responsabile della fornitura di risposte DNS autorevoli.
- Protezione contro i flussi di richieste a livello di applicazione Web. La regola basata sulla frequenza configurata nell'ACL AWS WAF Web blocca gli IP di origine quando inviano più richieste di quelle consentite dalla regola.

- Mitigazione automatica degli attacchi DDoS a livello di applicazione per le CloudFront distribuzioni, se scegli di abilitare questa opzione. Con la mitigazione automatica degli attacchi DDoS, Shield Advanced mantiene una regola basata sulla velocità nell'ACL AWS WAF web associato alla distribuzione che limita il volume di richieste provenienti da fonti DDoS note. Inoltre, quando Shield Advanced rileva un evento che influisce sullo stato dell'applicazione, crea, verifica e gestisce automaticamente le regole di mitigazione nell'ACL Web.
- Interazione proattiva con lo Shield Response Team (SRT), se scegli di abilitare questa opzione. Quando Shield Advanced rileva un evento che influisce sullo stato dell'applicazione, SRT risponde e interagisce in modo proattivo con i team di sicurezza o operativi utilizzando le informazioni di contatto fornite dall'utente. L'SRT analizza i modelli del traffico e può aggiornare le regole per bloccare l'attacco. AWS WAF

Esempio di resilienza DDoS per applicazioni TCP e UDP

Questo esempio mostra un'architettura resiliente agli attacchi DDoS per applicazioni TCP e UDP in una regione AWS che utilizza istanze Amazon Elastic Compute Cloud (Amazon EC2) o indirizzi Elastic IP (EIP).

Puoi seguire questo esempio generale per migliorare la resilienza DDoS per i seguenti tipi di applicazioni:

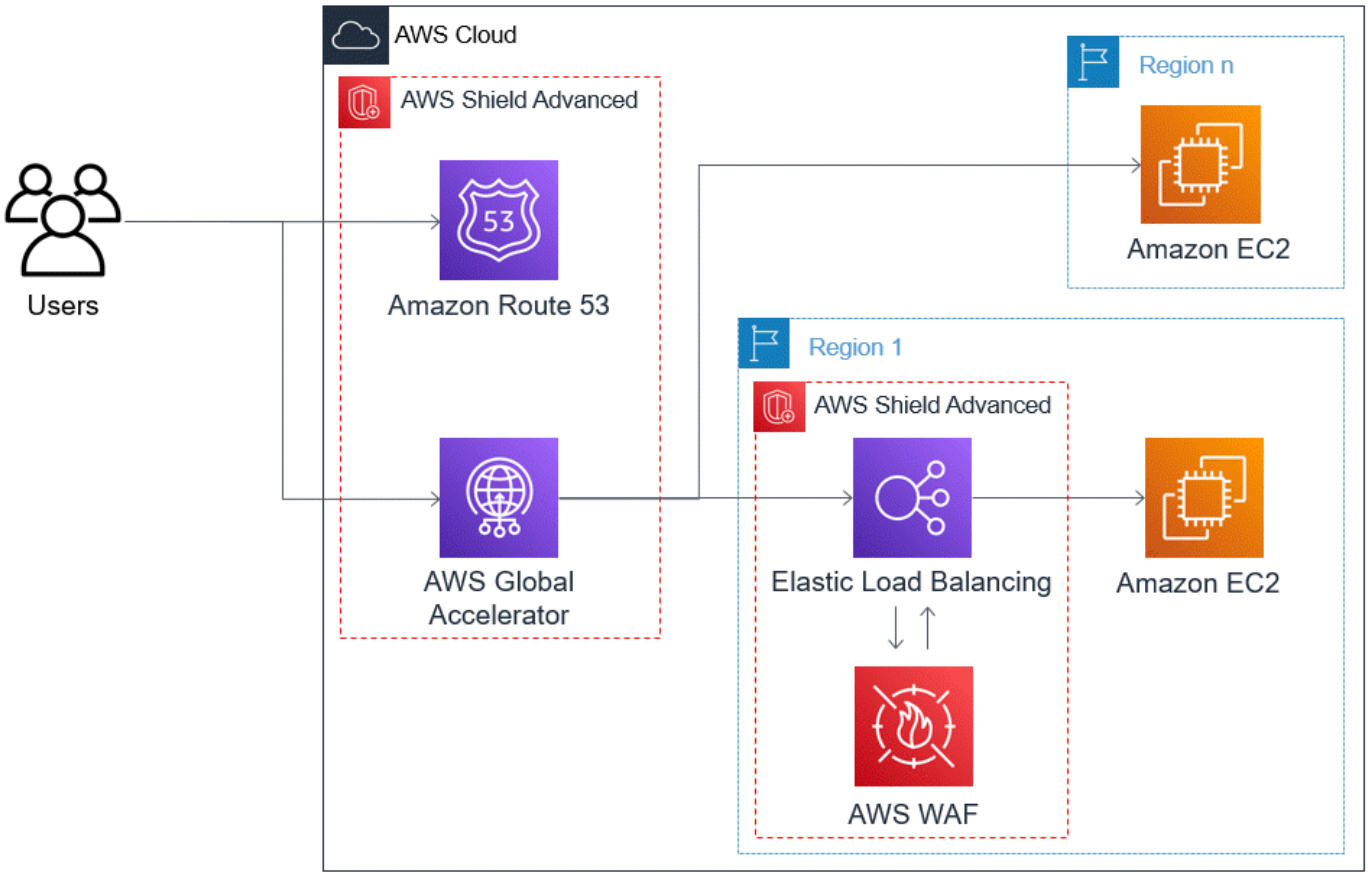
- Applicazioni TCP o UDP. Ad esempio, applicazioni utilizzate per giochi, IoT e voice over IP.
- Applicazioni Web che richiedono indirizzi IP statici o che utilizzano protocolli CloudFront non supportati da Amazon. Ad esempio, l'applicazione potrebbe richiedere indirizzi IP che gli utenti possono aggiungere agli elenchi di indirizzi consentiti dal firewall e che non vengono utilizzati da altri AWS clienti.

Puoi migliorare la resilienza DDoS per questi tipi di applicazioni introducendo Amazon Route 53 e. AWS Global Accelerator Questi servizi possono indirizzare gli utenti verso la tua applicazione e possono fornire all'applicazione indirizzi IP statici che vengono instradati in modalità anycast attraverso la AWS rete edge globale. Gli acceleratori standard Global Accelerator possono migliorare la latenza degli utenti fino al 60%. Se disponi di un'applicazione Web, puoi rilevare e mitigare i flood di richieste a livello di applicazione Web eseguendo l'applicazione su un Application Load Balancer e quindi proteggendo l'Application Load Balancer con un ACL Web. AWS WAF

Dopo aver creato l'applicazione, proteggi le zone ospitate di Route 53, gli acceleratori standard Global Accelerator e tutti gli Application Load Balancer con Shield Advanced. Quando proteggi i tuoi

Application Load Balancer, puoi associare ACL AWS WAF Web e creare relative regole basate sulla frequenza. Puoi configurare un coinvolgimento proattivo con SRT sia per gli acceleratori standard Global Accelerator che per gli Application Load Balancer associando controlli di integrità Route 53 nuovi o esistenti. Per ulteriori informazioni sulle opzioni, consulta. [Protezione delle risorse in AWS Shield Advanced]

Il seguente diagramma di riferimento illustra un esempio di architettura resiliente DDoS per applicazioni TCP e UDP.



I vantaggi che questo approccio offre alla tua applicazione includono i seguenti:

- Protezione contro gli attacchi DDoS più estesi conosciuti a livello di infrastruttura (livello 3 e livello 4). Se il volume di un attacco causa congestione a monte AWS, l'errore verrà isolato più vicino alla fonte e avrà un effetto minimo sugli utenti legittimi.
- Protezione dagli attacchi a livello di applicazione DNS, poiché Route 53 è responsabile della fornitura di risposte DNS autorevoli.

- Se disponi di un'applicazione Web, questo approccio fornisce protezione contro i flussi di richieste a livello di applicazione Web. La regola basata sulla frequenza configurata nell'ACL AWS WAF Web blocca gli IP di origine mentre inviano un numero di richieste superiore a quello consentito dalla regola.
- Interazione proattiva con lo Shield Response Team (SRT), se scegli di abilitare questa opzione per le risorse idonee. Quando Shield Advanced rileva un evento che influisce sullo stato dell'applicazione, SRT risponde e interagisce in modo proattivo con i team di sicurezza o operativi utilizzando le informazioni di contatto fornite dall'utente.

Esempi di casi d'uso di Shield Advanced

Puoi usare Shield Advanced per proteggere le tue risorse in molti tipi di scenari. Tuttavia, in alcuni casi è necessario utilizzare altri servizi o combinare altri servizi con Shield Advanced per offrire la migliore protezione. Di seguito sono riportati alcuni esempi di come utilizzare Shield Advanced o altri AWS servizi per proteggere le risorse.

Obiettivo	Servizi suggeriti	Documentazione servizi correlati
Proteggere un'applicazione Web e API RESTful da un attacco DDoS	Shield Advanced protegge una CloudFront distribuzione Amazon e un Application Load Balancer	Documentazione Elastic Load Balancing, documentazione Amazon CloudFront
Proteggere un'applicazione basata su TCP da un attacco DDoS	Shield Advanced protegge un acceleratore AWS Global Accelerator standard; collegato a un indirizzo IP elastico	AWS Global Accelerator Documentazione, documentazione Elastic Load Balancing
Proteggere un server di gioco basato su UDP da un attacco DDoS	Shield Advanced protegge un'istanza Amazon EC2 collegata a un indirizzo IP elastico	Amazon Elastic Compute Cloud Documentation

Ad esempio, se si utilizza Shield Advanced per proteggere un indirizzo IP elastico, Shield Advanced protegge qualsiasi risorsa ad esso associata. Durante un attacco, Shield Advanced distribuisce automaticamente gli ACL di rete ai confini della AWS rete. Quando gli ACL di rete si trovano ai margini della rete, Shield Advanced può fornire protezione da eventi DDoS di grandi dimensioni. In genere, gli ACL di rete vengono applicati vicino alle istanze Amazon EC2 all'interno di Amazon VPC. L'ACL di rete può mitigare gli attacchi solo se il tuo Amazon VPC e la tua istanza sono in grado di gestire. Se l'interfaccia di rete collegata all'istanza Amazon EC2 è in grado di elaborare fino a 10 Gbps, i volumi superiori a 10 Gbps rallentano e possono bloccare il traffico verso quell'istanza. Durante un attacco, Shield Advanced promuove l'ACL di rete fino al AWS confine, che può elaborare più terabyte di traffico. La lista di controllo degli accessi di rete è in grado di fornire protezione per le risorse ben oltre la capacità tipica della rete. Per ulteriori informazioni sulle liste di controllo degli accessi di rete, consulta l'articolo relativo alle liste di controllo degli accessi di rete.

Iniziare con AWS Shield Advanced

Questo tutorial illustra come iniziare a AWS Shield Advanced utilizzare la console Shield Advanced.

> **Note**
>
> Shield Advanced richiede un abbonamento, mentre AWS Shield Standard non lo richiede. Le protezioni fornite da Shield Standard sono disponibili gratuitamente per tutti i AWS clienti.

Shield Advanced offre una protezione avanzata di rilevamento e mitigazione degli attacchi DDoS per gli attacchi a livello di rete (livello 3), livello di trasporto (livello 4) e livello di applicazione (livello 7). Per ulteriori informazioni su Shield Advanced, vedereAWS Shield Advanced panoramica.

La comunità AWS tecnica ha pubblicato informazioni su un esempio di opzione con un clic per l'utilizzo AWS CloudFormation e AWS Firewall Manager la configurazione di Shield Advanced. Puoi utilizzare Firewall Manager se i tuoi account fanno parte di un'organizzazione in AWS Organizations e se stai proteggendo qualsiasi tipo di risorsa ad eccezione di Amazon Route 53 o AWS Global Accelerator. Per esplorare questa opzione, consulta il tutorial in Implementazione con un clic di Shield Advanced.

> **Note**
>
> È importante configurare completamente Shield Advanced prima di un evento Distributed Denial of Service (DDoS). Completa la configurazione per garantire che l'applicazione sia protetta e che tu sia pronto a rispondere in caso di attacco DDoS.

Eseguire le seguenti fasi in sequenza.

Indice

Iscriviti a AWS Shield Advanced

È necessario abbonarsi a Shield Advanced per ognuno di essi Account AWS che si desidera proteggere. Non è necessario abbonarsi a Shield Standard.

Fatturazione dell'abbonamento Shield Advanced

Se sei un AWS Channel Reseller, contatta il team del tuo account per informazioni e assistenza. Queste informazioni di fatturazione sono destinate ai clienti che non sono rivenditori di AWS canale.

Per tutti gli altri, si applicano le seguenti linee guida per l'abbonamento e la fatturazione:

- Per gli account membri di un' AWS Organizations organizzazione, AWS addebita gli abbonamenti Shield Advanced sul conto pagante dell'organizzazione, indipendentemente dal fatto che l'account di pagamento stesso sia sottoscritto.
- Quando sottoscrivi più account appartenenti alla stessa famiglia di conti di fatturazione AWS Organizations consolidati, un unico prezzo di abbonamento copre tutti gli account sottoscritti della famiglia. L'organizzazione deve possedere tutte Account AWS e tutte le proprie risorse.

- Quando sottoscrivi più account per più organizzazioni, puoi comunque pagare un'unica quota di abbonamento per tutte le organizzazioni, gli account e le risorse, purché tu ne sia il proprietario. Contatta il tuo account manager o l' AWS assistenza e richiedi un'esenzione dai costi di AWS Shield Advanced abbonamento per tutte le organizzazioni tranne una.

Per informazioni dettagliate ed esempi sui prezzi, consulta AWS Shield Prezzi.

Semplifica gli abbonamenti con AWS Firewall Manager

Se i tuoi account fanno parte di un'organizzazione, ti consigliamo di utilizzarli, AWS Firewall Manager se possibile, per automatizzare gli abbonamenti e le protezioni per l'organizzazione. Firewall Manager supporta tutti i tipi di risorse protette ad eccezione di Amazon Route 53 e AWS Global Accelerator. Per utilizzare Firewall Manager, vedere AWS Firewall Manager eGuida introduttiva alle AWS Firewall ManagerAWS Shield Advanced politiche.

Se non utilizzi Firewall Manager, per ogni account con risorse da proteggere, sottoscrivi e aggiungi protezioni utilizzando le seguenti procedure.

Per sottoscrivere un account a AWS Shield Advanced

1. Accedi AWS Management Console e apri la console AWS WAF & Shield all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nella barra AWS Shielddi navigazione, scegli Guida introduttiva. Scegli Iscriviti a Shield Advanced.
3. Nella pagina Iscriviti a Shield Advanced, leggi ogni termine del contratto, quindi seleziona tutte le caselle di controllo per indicare che accetti i termini. Per gli account appartenenti a un gruppo di fatturazione consolidato, devi accettare i termini di ciascun account.

   > **Important**
   >
   > Quando sei abbonato, per annullare l'iscrizione devi contattare. AWS Support Per disabilitare il rinnovo automatico dell'abbonamento, è necessario utilizzare l'operazione Shield API o il comando UpdateSubscriptionCLI update-subscription.

   Scegli Iscriviti a Shield Advanced. Questo sottoscrive il tuo account a Shield Advanced e attiva il servizio.

Il tuo account è abbonato. Continua con i seguenti passaggi per proteggere le risorse del tuo account con Shield Advanced.

> **Note**
>
> Shield Advanced non protegge automaticamente le tue risorse dopo l'iscrizione. È necessario specificare le risorse che si desidera proteggere da Shield Advanced e configurare le protezioni.

Aggiungi risorse per proteggere e configurare le protezioni

Shield Advanced protegge solo le risorse specificate, tramite Shield Advanced o in una politica Firewall Manager Shield Advanced. Non protegge automaticamente le risorse di un account sottoscritto.

Se utilizzi una politica AWS Firewall Manager Shield Advanced per le tue protezioni, non è necessario eseguire questo passaggio. La policy viene configurata con i tipi di risorse da proteggere e Firewall Manager aggiunge automaticamente protezioni alle risorse che rientrano nell'ambito della policy.

Se non utilizzi Firewall Manager, segui le seguenti procedure per ogni account che dispone di risorse da proteggere.

Per scegliere le risorse da proteggere utilizzando Shield Advanced

1. Scegli Aggiungi risorse da proteggere dalla pagina di conferma dell'abbonamento della procedura precedente o dalla pagina Risorse protette o Panoramica.
2. Nella pagina Scegli le risorse da proteggere con Shield Advanced, in Specificare l'area e i tipi di risorse, fornisci le specifiche della regione e del tipo di risorsa per le risorse che desideri proteggere. È possibile proteggere le risorse in più regioni selezionando Tutte le regioni e restringere la selezione alle risorse globali selezionando Globale. È possibile deselezionare tutti i tipi di risorse che non si desidera proteggere. Per informazioni sulle protezioni per i tipi di risorse, consulta. AWS Shield Advanced protezioni per tipo di risorsa
3. Scegli Carica risorse. Shield Advanced compila la sezione Seleziona risorse con le AWS risorse che corrispondono ai tuoi criteri.
4. Nella sezione Seleziona risorse, puoi filtrare l'elenco delle risorse inserendo una stringa da cercare negli elenchi delle risorse.

Seleziona le risorse che desideri proteggere.

5. Nella sezione Tag, se desideri aggiungere tag alle protezioni Shield Advanced che stai creando, specificali. Per informazioni sull'etichettatura AWS delle risorse, consulta Lavorare con Tag Editor.
6. Scegli Proteggi con Shield Advanced. Ciò aggiunge le protezioni Shield Advanced alle risorse.

Continua attraverso le schermate della procedura guidata della console per completare la configurazione delle protezioni delle risorse.

Argomenti

- Configura le protezioni DDoS a livello applicativo (livello 7) con AWS WAF
- Configura il rilevamento basato sulla salute per le tue protezioni
- Configurazione di allarmi e notifiche
- Rivedi e completa la configurazione della protezione

Configura le protezioni DDoS a livello applicativo (livello 7) con AWS WAF

Per proteggere una risorsa a livello di applicazione, Shield Advanced utilizza un ACL AWS WAF Web con una regola basata sulla velocità come punto di partenza. AWS WAF è un firewall per applicazioni Web che consente di monitorare le richieste HTTP e HTTPS inoltrate alle risorse del livello applicativo e consente di controllare l'accesso ai contenuti in base alle caratteristiche delle richieste. Una regola basata sulla frequenza limita il volume del traffico in base ai criteri di aggregazione delle richieste, fornendo una protezione DDoS di base all'applicazione. Per ulteriori informazioni, consultare Come AWS WAF funziona e Istruzione regola basata sulla frequenza.

Se lo desideri, puoi anche abilitare la mitigazione automatica degli attacchi DDoS a livello di applicazione Shield Advanced, in modo che Shield Advanced limiti la frequenza delle richieste provenienti da fonti DDoS note e fornisca automaticamente protezioni specifiche in base agli incidenti.

> **Important**
>
> Se gestisci le tue protezioni Shield Advanced AWS Firewall Manager utilizzando una policy Shield Advanced, non puoi gestire le protezioni a livello di applicazione qui. È necessario gestirli nella politica Firewall Manager Shield Advanced.

Abbonamenti e AWS WAF costi Shield Advanced

L'abbonamento a Shield Advanced copre i costi di utilizzo delle AWS WAF funzionalità standard per le risorse che proteggi con Shield Advanced. AWS WAF Le tariffe standard coperte dalle protezioni Shield Advanced sono il costo per ACL Web, il costo per regola e il prezzo base per milione di richieste per l'ispezione delle richieste Web, fino a 1.500 WCU e fino alla dimensione corporea predefinita.

L'attivazione della mitigazione automatica degli attacchi DDoS a livello di applicazione Shield Advanced aggiunge un gruppo di regole all'ACL Web che utilizza 150 unità di capacità ACL Web (WCU). Queste WCU influiscono sull'utilizzo della WCU nell'ACL web. Per ulteriori informazioni, consulta Mitigazione DDoS automatica a livello di applicazione Shield Advanced, Il gruppo di regole Shield Advanced e AWS WAF unità di capacità Web ACL (WCU).

L'abbonamento a Shield Advanced non copre l'uso AWS WAF di risorse che non proteggi utilizzando Shield Advanced. Inoltre, non copre eventuali AWS WAF costi aggiuntivi non standard per le risorse protette. Esempi di AWS WAF costi non standard sono quelli per Bot Control, per l'azione delle CAPTCHA regole, per gli ACL Web che utilizzano più di 1.500 WCU e per l'ispezione del corpo della richiesta oltre le dimensioni corporee predefinite. L'elenco completo è disponibile nella pagina dei prezzi. AWS WAF

Per informazioni complete ed esempi di prezzi, consulta la pagina Prezzi e AWS WAF prezzi di Shield.

Per configurare le protezioni DDoS di livello 7 per una regione

Shield Advanced offre la possibilità di configurare la mitigazione degli attacchi DDoS di livello 7 per ogni regione in cui si trovano le risorse scelte. Se stai aggiungendo protezioni in più regioni, la procedura guidata ti guida attraverso la seguente procedura per ciascuna regione.

1. La pagina Configura le protezioni DDoS di livello 7 elenca tutte le risorse che non sono ancora associate a un ACL Web. Per ognuna di queste, scegli un ACL web esistente o crea un nuovo ACL web. Per qualsiasi risorsa a cui è già associato un ACL Web, puoi modificare gli ACL Web dissociando prima quello corrente. AWS WAF Per ulteriori informazioni, consulta Associazione o dissociazione di un ACL Web con una risorsa AWS.

   Per gli ACL Web che non dispongono già di una regola basata sulla frequenza, la procedura guidata di configurazione richiede di aggiungerne una. Una regola basata sulla frequenza limita il traffico proveniente dagli indirizzi IP quando inviano un volume elevato di richieste. Le regole

basate sulla frequenza aiutano a proteggere l'applicazione dai flussi di richieste Web e possono fornire avvisi in caso di picchi improvvisi di traffico che potrebbero indicare un potenziale attacco DDoS. Aggiungi una regola basata sulla velocità a un ACL Web selezionando Aggiungi regola limite di velocità e quindi specificando un limite di velocità e un'azione per la regola. È possibile configurare protezioni aggiuntive nell'ACL Web tramite. AWS WAF

Per informazioni sull'utilizzo degli ACL Web e delle regole basate sulla tariffa nelle protezioni Shield Advanced, incluse opzioni di configurazione aggiuntive per le regole basate sulla tariffa, consulta. ACL AWS WAF Web Shield Advanced a livello applicativo e regole basate sulla velocità

2. Per la mitigazione automatica degli attacchi DDoS a livello di applicazione, se desideri che Shield Advanced mitighi automaticamente gli attacchi DDoS contro le risorse del livello di applicazione, scegli Abilita e quindi seleziona l'azione della AWS WAF regola che desideri che Shield Advanced utilizzi nelle sue regole personalizzate. Questa impostazione si applica a tutti gli ACL Web per le risorse gestite in questa sessione guidata.

   Con la mitigazione automatica degli attacchi DDoS a livello di applicazione, Shield Advanced mantiene una regola basata sulla frequenza nell'ACL AWS WAF web della risorsa che limita il volume di richieste provenienti da fonti DDoS note. Inoltre, Shield Advanced confronta i modelli di traffico attuali con le linee di base del traffico storico per rilevare deviazioni che potrebbero indicare un attacco DDoS. Quando Shield Advanced rileva un attacco DDoS, risponde creando, valutando e implementando regole personalizzate per rispondere. AWS WAF Sei tu a specificare se le regole personalizzate contano o bloccano gli attacchi per tuo conto.

   > **Note**
   >
   > La mitigazione automatica degli attacchi DDoS a livello di applicazione funziona solo con gli ACL Web creati utilizzando l'ultima versione di AWS WAF (v2).

   Per ulteriori informazioni sulla mitigazione automatica degli attacchi DDoS a livello di applicazione Shield Advanced, comprese le avvertenze e le migliori pratiche per l'utilizzo di questa funzionalità, vedere. Mitigazione DDoS automatica a livello di applicazione Shield Advanced

3. Seleziona Successivo. La procedura guidata della console passa alla pagina di rilevamento basata sullo stato di salute.

Configura il rilevamento basato sulla salute per le tue protezioni

Configura Shield Advanced per utilizzare il rilevamento basato sullo stato di salute per migliorare la reattività e la precisione nel rilevamento e nella mitigazione degli attacchi. Controlli sanitari ben configurati sono essenziali per un rilevamento accurato degli eventi. È possibile configurare il rilevamento basato sullo stato di salute per qualsiasi tipo di risorsa ad eccezione delle zone ospitate su Route 53.

Per utilizzare il rilevamento basato sullo stato, definisci un controllo dello stato della tua risorsa in Route 53, quindi associa il controllo dello stato alla protezione Shield Advanced. È importante che il controllo dello stato che configuri rifletta accuratamente lo stato della risorsa. Per informazioni ed esempi sulla configurazione dei controlli sanitari da utilizzare con Shield Advanced, vedereRilevamento basato sulla salute mediante controlli sanitari.

I controlli Health sono necessari per il supporto proattivo al coinvolgimento dello Shield Response Team (SRT). Per informazioni sul coinvolgimento proattivo, consulta. Configurazione del coinvolgimento proattivo

> **Note**
>
> I controlli Health devono essere considerati sani quando vengono associati alle protezioni Shield Advanced.

Per configurare il rilevamento basato sullo stato di salute

1. In Associated Health Check (Controllo stato associato), scegliere l'ID del controllo dello stato che si desidera associare alla protezione.

   > **Note**
   >
   > Se non vedi il controllo sanitario di cui hai bisogno, vai alla console Route 53 e verifica il controllo e il relativo ID. Per informazioni, consultare Creazione e aggiornamento di controlli dello stato.

2. Seleziona Successivo. La procedura guidata della console passa alla pagina degli allarmi e delle notifiche.

Configurazione di allarmi e notifiche

Facoltativamente, puoi configurare le notifiche di Amazon Simple Notification Service per gli CloudWatch allarmi Amazon rilevati e l'attività delle regole basate sulla tariffa. È possibile utilizzarli per ricevere notifiche quando Shield rileva un evento su una risorsa protetta o quando viene superato un limite di velocità configurato in una regola basata sulla velocità.

Per informazioni sulle CloudWatch metriche Shield Advanced, consultaAWS Shield Advanced metriche. Per informazioni su Amazon SNS, consulta la Amazon Simple Notification Service Developer Guide.

Per configurare allarmi e notifiche

1. Seleziona gli argomenti di Amazon SNS per i quali desideri ricevere la notifica. Puoi utilizzare un unico argomento di Amazon SNS per tutte le risorse protette e le regole basate sulle tariffe oppure puoi scegliere argomenti diversi, personalizzati in base alla tua organizzazione. Ad esempio, puoi creare un argomento SNS per ogni team responsabile della risposta agli incidenti per un set specifico di risorse.
2. Seleziona Successivo. La procedura guidata della console passa alla pagina di revisione della protezione delle risorse.

Rivedi e completa la configurazione della protezione

Per rivedere e configurare le impostazioni

1. Nella pagina Rivedi e configura la mitigazione e la visibilità degli attacchi DDoS, rivedi le tue impostazioni. Per apportare modifiche, scegli Modifica nell'area che desideri modificare. In questo modo si torna alla pagina associata nella procedura guidata della console. Apporta le modifiche, quindi scegli Avanti nelle pagine successive fino a tornare alla pagina Rivedi e configura la mitigazione e la visibilità degli attacchi DDoS.
2. Scegli Termina configurazione. La pagina Risorse protette elenca le nuove risorse protette.

Configurare il AWS supporto SRT

Lo Shield Response Team (SRT) sono ingegneri della sicurezza specializzati nella risposta agli eventi DDoS. Facoltativamente, puoi aggiungere autorizzazioni che consentono all'SRT di gestire le risorse per tuo conto durante un evento DDoS. Inoltre, puoi configurare l'SRT per interagire in

modo proattivo se i controlli di integrità della Route 53 associati alle tue risorse protette non sono funzionanti durante un evento rilevato. Entrambe queste aggiunte alle protezioni consentono risposte più rapide agli eventi DDoS.

> **Note**
>
> Per utilizzare i servizi dello Shield Response Team (SRT), è necessario essere abbonati al piano Business Support o al piano Enterprise Support.

L'SRT può monitorare i dati e i registri delle AWS WAF richieste durante gli eventi a livello di applicazione per identificare il traffico anomalo. Possono aiutare a creare AWS WAF regole personalizzate per mitigare le fonti di traffico offensive. Se necessario, l'SRT potrebbe formulare raccomandazioni architettoniche per aiutarvi ad allineare meglio le vostre risorse ai consigli. AWS

Per ulteriori informazioni sull'SRT, vedere. Supporto dello Shield Response Team (SRT)

Per concedere le autorizzazioni all'SRT

1. Nella pagina Panoramica della AWS Shield console, in Configura supporto AWS SRT, scegli Modifica accesso SRT. Viene visualizzata la pagina di accesso Edit AWS Shield Response Team (SRT).
2. Per l'impostazione dell'accesso SRT, selezionate una delle opzioni:

   - Non concedere a SRT l'accesso al mio account: Shield rimuove tutte le autorizzazioni che hai precedentemente concesso all'SRT per accedere al tuo account e alle tue risorse.
   - Crea un nuovo ruolo per l'SRT per accedere al mio account: Shield crea un ruolo che si fida del responsabile del servizio`drt.shield.amazonaws.com`, che rappresenta l'SRT, e gli allega la policy gestita. `AWSShieldDRTAccessPolicy` La policy gestita consente all'SRT di effettuare chiamate AWS WAF API per vostro conto AWS Shield Advanced e di accedere ai vostri log. AWS WAF Per ulteriori informazioni sulla policy gestita, consulta AWS politica gestita: AWSShieldDRTAccessPolicy.
   - Scegli un ruolo esistente per l'SRT per accedere ai miei account: per questa opzione, devi modificare la configurazione del ruolo in AWS Identity and Access Management (IAM) come segue:
     - Collegare la policy gestita `AWSShieldDRTAccessPolicy` al ruolo. Questa politica gestita consente all'SRT di effettuare AWS Shield Advanced chiamate AWS WAF API per vostro conto e di accedere ai vostri AWS WAF log. Per ulteriori informazioni sulla policy gestita,

consulta AWS politica gestita: AWSShieldDRTAccessPolicy. Per informazioni su come allegare la policy gestita al tuo ruolo, consulta Allegare e scollegare le politiche IAM.

- Modificare il ruolo per considerare attendibile il principale del servizio `drt.shield.amazonaws.com`. Questo è il servizio principale che rappresenta l'SRT. Per ulteriori informazioni, consulta Elementi della policy JSON di IAM: Principal.

3. Scegliere Salva per salvare le modifiche.

Per ulteriori informazioni su come concedere all'SRT l'accesso alle tue protezioni e ai tuoi dati, consulta. Configurazione dell'accesso per lo Shield Response Team (SRT)

Per abilitare il coinvolgimento proattivo di SRT

1. Nella pagina Panoramica della AWS Shield console, in Coinvolgimento proattivo e contatti, nell'area contatti, scegli Modifica.

   Nella pagina Modifica contatti, fornisci le informazioni di contatto per le persone che desideri che SRT contatti per un coinvolgimento proattivo.

   Se fornisci più di un contatto, nelle Note, indica le circostanze in cui ogni contatto deve essere utilizzato. Includi le designazioni dei contatti principali e secondari e fornisci gli orari di disponibilità e i fusi orari di ogni contatto.

   Note di contatto di esempio:

   - Questa è una hotline con personale 24 ore su 24, 7 giorni su 7, 365 giorni l'anno. Collabora con l'analista incaricato della risposta e troverà la persona appropriata per la chiamata.
   - Contattatemi se la hotline non risponde entro 5 minuti.

2. Selezionare Salva.

   La pagina Panoramica riporta le informazioni di contatto aggiornate.

3. Scegli Modifica la funzione di coinvolgimento proattivo, scegli Abilita, quindi scegli Salva per abilitare il coinvolgimento proattivo.

Per ulteriori informazioni sul coinvolgimento proattivo, consulta. Configurazione del coinvolgimento proattivo

Crea una dashboard DDoS CloudWatch e imposta gli allarmi CloudWatch

Puoi monitorare le potenziali attività DDoS utilizzando Amazon CloudWatch, che raccoglie dati grezzi da Shield Advanced e li elabora in metriche leggibili quasi in tempo reale. Puoi utilizzare le statistiche CloudWatch per avere una prospettiva sulle prestazioni della tua applicazione o del tuo servizio web. Per ulteriori informazioni sull'utilizzo CloudWatch, consulta What is CloudWatch in the Amazon CloudWatch User Guide.

- Per istruzioni sulla creazione di una CloudWatch dashboard, consultaMonitoraggio con Amazon CloudWatch.
- Per le descrizioni delle metriche Shield Advanced che puoi aggiungere alla dashboard, consultaAWS Shield Advanced metriche.

Shield Advanced riporta le metriche delle risorse con CloudWatch maggiore frequenza durante gli eventi DDoS rispetto a quando non è in corso alcun evento. Shield Advanced riporta le metriche una volta al minuto durante un evento e poi una volta subito dopo la fine dell'evento. Sebbene non sia in corso alcun evento, Shield Advanced riporta le metriche una volta al giorno, all'ora assegnata alla risorsa. Questo rapporto periodico mantiene le metriche attive e disponibili per l'uso negli allarmi personalizzati. CloudWatch

Questo completa il tutorial per iniziare a usare Shield Advanced. Per sfruttare appieno le protezioni che hai scelto, continua a esplorare le funzionalità e le opzioni di Shield Advanced. Per iniziare, acquisisci familiarità con le opzioni a tua disposizione per visualizzare e rispondere agli eventi in tempo reale. Visibilità sugli eventi DDoS Risposta agli eventi DDoS

Supporto dello Shield Response Team (SRT)

Lo Shield Response Team (SRT) fornisce ulteriore supporto per i clienti Shield Advanced. Gli SRT sono ingegneri della sicurezza specializzati nella risposta agli eventi DDoS. Come ulteriore livello di supporto al vostro AWS Support piano, potete lavorare direttamente con l'SRT, sfruttando la loro esperienza come parte del flusso di lavoro di risposta agli eventi. Per informazioni sulle opzioni e per indicazioni sulla configurazione, consultate gli argomenti seguenti.

> **Note**
>
> Per utilizzare i servizi dello Shield Response Team (SRT), è necessario essere abbonati al piano Business Support o al piano Enterprise Support.

Attività di supporto SRT

L'obiettivo principale di una collaborazione con SRT è proteggere la disponibilità e le prestazioni dell'applicazione. A seconda del tipo di evento DDoS e dell'architettura dell'applicazione, l'SRT può eseguire una o più delle seguenti azioni:

- AWS WAF analisi e regole dei log: per le risorse che utilizzano un ACL AWS WAF web, SRT può analizzare AWS WAF i log per identificare le caratteristiche di attacco nelle richieste web dell'applicazione. Con la vostra approvazione durante l'attivazione, l'SRT può applicare modifiche all'ACL web per bloccare gli attacchi che ha identificato.
- Crea mitigazioni di rete personalizzate: l'SRT può scrivere mitigazioni personalizzate per gli attacchi a livello di infrastruttura. L'SRT può collaborare con voi per comprendere il traffico previsto per la vostra applicazione, bloccare il traffico imprevisto e ottimizzare i limiti di frequenza dei pacchetti al secondo. Per ulteriori informazioni, consulta Configurazione di mitigazioni personalizzate con lo Shield Response Team (SRT).
- Ingegneria del traffico di rete: SRT collabora a stretto contatto con i team AWS di rete per proteggere i clienti di Shield Advanced. Se necessario, AWS può modificare il modo in cui il traffico Internet arriva sulla AWS rete per allocare una maggiore capacità di mitigazione all'applicazione.
- Raccomandazioni sull'architettura: l'SRT può stabilire che la migliore mitigazione di un attacco richieda modifiche all'architettura per allinearsi meglio alle AWS migliori pratiche e contribuirà a supportare l'implementazione di queste pratiche. Per informazioni, consulta AWS Best Practices for DDoS Resiliency.

Argomenti

Configurazione dell'accesso per lo Shield Response Team (SRT)

Puoi concedere l'autorizzazione allo Shield Response Team (SRT) di agire per tuo conto, accedere ai tuoi AWS WAF registri ed effettuare chiamate alle AWS WAF API AWS Shield Advanced e per gestire le protezioni. Durante gli eventi DDoS a livello applicativo, l'SRT può monitorare AWS WAF

le richieste per identificare il traffico anomalo e contribuire alla creazione di regole personalizzate per mitigare le fonti di traffico pericolose. AWS WAF

Inoltre, puoi concedere all'SRT l'accesso ad altri dati che hai archiviato nei bucket Amazon S3, come acquisizioni di pacchetti o log da un Application Load Balancer, CloudFront Amazon o da fonti di terze parti.

> **Note**
>
> Per utilizzare i servizi dello Shield Response Team (SRT), è necessario essere abbonati al piano Business Support o al piano Enterprise Support.

Per gestire le autorizzazioni per l'SRT

1. Nella pagina Panoramica della AWS Shield console, in Configura supporto AWS SRT, scegli Modifica accesso SRT. Viene visualizzata la pagina di accesso Edit AWS Shield Response Team (SRT).
2. Per l'impostazione dell'accesso SRT, selezionate una delle opzioni:
   - Non concedere a SRT l'accesso al mio account: Shield rimuove tutte le autorizzazioni che hai precedentemente concesso all'SRT per accedere al tuo account e alle tue risorse.
   - Crea un nuovo ruolo per l'SRT per accedere al mio account: Shield crea un ruolo che si fida del responsabile del servizio`drt.shield.amazonaws.com`, che rappresenta l'SRT, e gli allega la policy gestita. `AWSShieldDRTAccessPolicy` La policy gestita consente all'SRT di effettuare chiamate AWS WAF API per vostro conto AWS Shield Advanced e di accedere ai vostri log. AWS WAF Per ulteriori informazioni sulla policy gestita, consulta AWS politica gestita: AWSShieldDRTAccessPolicy.
   - Scegli un ruolo esistente per l'SRT per accedere ai miei account: per questa opzione, devi modificare la configurazione del ruolo in AWS Identity and Access Management (IAM) come segue:
     - Collegare la policy gestita `AWSShieldDRTAccessPolicy` al ruolo. Questa politica gestita consente all'SRT di effettuare AWS Shield Advanced chiamate AWS WAF API per vostro conto e di accedere ai vostri AWS WAF log. Per ulteriori informazioni sulla policy gestita, consulta AWS politica gestita: AWSShieldDRTAccessPolicy. Per informazioni su come allegare la policy gestita al tuo ruolo, consulta Allegare e scollegare le politiche IAM.

- Modificare il ruolo per considerare attendibile il principale del servizio `drt.shield.amazonaws.com`. Questo è il servizio principale che rappresenta l'SRT. Per ulteriori informazioni, consulta Elementi della policy JSON di IAM: Principal.

3. Per (Facoltativo): concedi l'accesso SRT a un bucket Amazon S3, se devi condividere dati che non si trovano nei AWS WAF tuoi log ACL Web, configuralo. Ad esempio, i log di accesso di Application Load Balancer, i log di Amazon o CloudFront i log provenienti da fonti di terze parti.

> **Note**
>
> Non è necessario eseguire questa operazione per i log ACL Web AWS WAF . L'SRT ottiene l'accesso a questi dati quando concedi l'accesso al tuo account.

   a. Configura i bucket Amazon S3 in base alle seguenti linee guida:

      - Le posizioni dei bucket devono essere le Account AWS stesse a cui hai concesso l'accesso generale all'SRT, nel passaggio precedente per l'accesso allo AWS Shield Response Team (SRT).
      - I bucket possono essere in testo semplice o crittografati con SSE-S3. Per ulteriori informazioni sulla crittografia SSE-S3 di Amazon S3, consulta Protezione dei dati utilizzando la crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3) nella Guida per l'utente di Amazon S3.

        L'SRT non può visualizzare o elaborare i log archiviati in bucket crittografati con chiavi archiviate in (). AWS Key Management Service AWS KMS

   b. Nella sezione Shield Advanced (opzionale): concedi l'accesso SRT a un bucket Amazon S3, per ogni bucket Amazon S3 in cui sono archiviati i dati o i log, inserisci il nome del bucket e scegli Aggiungi bucket. È possibile aggiungere fino a 10 bucket.

      Ciò concede all'SRT le seguenti autorizzazioni per ogni bucket:, e. `s3:GetBucketLocation` `s3:GetObject` `s3:ListBucket`

      Se desideri concedere all'SRT l'autorizzazione ad accedere a più di 10 bucket, puoi farlo modificando le politiche aggiuntive del bucket e concedendo manualmente le autorizzazioni elencate qui per l'SRT.

      Di seguito viene mostrato un elenco di politiche di esempio.

```
{
    "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. Scegliere Salva per salvare le modifiche.

È inoltre possibile autorizzare l'SRT tramite l'API creando un ruolo IAM, allegandovi la policy e quindi passando il ruolo AWSShieldDRTAccessPolicy all'operazione AssociateDRTRole.

Configurazione del coinvolgimento proattivo

Con un coinvolgimento proattivo, lo Shield Response Team (SRT) contatta direttamente l'utente quando la disponibilità o le prestazioni dell'applicazione sono compromesse da un possibile attacco. Consigliamo questo modello di coinvolgimento perché fornisce la risposta SRT più rapida e consente all'SRT di iniziare la risoluzione dei problemi anche prima di stabilire un contatto con voi.

L'engagement proattivo è disponibile per gli eventi a livello di rete e trasporto su indirizzi IP elastici e acceleratori AWS Global Accelerator standard e per i flussi di richieste Web sulle distribuzioni Amazon e sugli Application Load Balancer. CloudFront Il coinvolgimento proattivo è disponibile solo per le protezioni delle risorse Shield Advanced a cui è associato un controllo dello stato di Amazon Route 53. Per informazioni sulla gestione e l'utilizzo dei controlli sanitari, consulta. Rilevamento basato sulla salute mediante controlli sanitari

Durante un evento rilevato da Shield Advanced, l'SRT utilizza lo stato dei controlli sullo stato di salute per determinare se l'evento è idoneo per un coinvolgimento proattivo. In tal caso, l'SRT vi contatterà in base alle indicazioni di contatto fornite nella configurazione del coinvolgimento proattivo.

Puoi configurare fino a dieci contatti per un coinvolgimento proattivo e puoi fornire note per aiutare l'SRT a contattarti. I vostri contatti proattivi dovrebbero essere disponibili per interagire con l'SRT durante gli eventi. Se non disponi di un centro operativo aperto 24 ore su 24, 7 giorni su 7, puoi fornire un contatto tramite cercapersone e indicare questa preferenza di contatto nelle tue note di contatto.

Il coinvolgimento proattivo richiede che tu faccia quanto segue:

- È necessario essere abbonati al piano Business Support o al piano Enterprise Support.
- Devi associare un controllo dello stato di Amazon Route 53 a qualsiasi risorsa che desideri proteggere con un coinvolgimento proattivo. L'SRT utilizza lo stato dei controlli sanitari per determinare se un evento richiede un coinvolgimento proattivo, quindi è importante che i controlli sanitari riflettano accuratamente lo stato delle risorse protette. Per ulteriori informazioni e indicazioni, vedere. Rilevamento basato sulla salute mediante controlli sanitari
- Per una risorsa a cui è associato un ACL AWS WAF Web, è necessario creare l'ACL Web utilizzando AWS WAF (v2), che è la versione più recente di. AWS WAF
- È necessario fornire almeno un contatto affinché l'SRT possa utilizzare per un coinvolgimento proattivo durante un evento. Mantieni le tue informazioni di contatto complete e aggiornate.

Per consentire un coinvolgimento proattivo SRT

1. Nella pagina Panoramica della AWS Shield console, in Coinvolgimento proattivo e contatti, nell'area contatti, scegli Modifica.

   Nella pagina Modifica contatti, fornisci le informazioni di contatto per le persone che desideri che SRT contatti per un coinvolgimento proattivo.

   Se fornisci più di un contatto, nelle Note, indica le circostanze in cui ogni contatto deve essere utilizzato. Includi le designazioni dei contatti principali e secondari e fornisci gli orari di disponibilità e i fusi orari di ogni contatto.

   Note di contatto di esempio:

   - Questa è una hotline con personale 24 ore su 24, 7 giorni su 7, 365 giorni l'anno. Collabora con l'analista incaricato della risposta e troverà la persona appropriata per la chiamata.
   - Contattatemi se la hotline non risponde entro 5 minuti.
2. Selezionare Salva.

La pagina Panoramica riporta le informazioni di contatto aggiornate.

3. Scegli Modifica la funzione di coinvolgimento proattivo, scegli Abilita, quindi scegli Salva per abilitare il coinvolgimento proattivo.

Contattare lo Shield Response Team (SRT)

Puoi contattare lo Shield Response Team (SRT) in uno dei seguenti modi:

Caso di supporto

Puoi aprire una custodia AWS Shieldnella console del AWS Support Center.

Per indicazioni sulla creazione di una richiesta di assistenza, consulta il AWS Support Centro.

Seleziona la gravità appropriata alla tua situazione e fornisci i tuoi dati di contatto. Nella descrizione, fornisci quanti più dettagli possibile. Fornisci informazioni su eventuali risorse protette che ritieni possano essere interessate e sullo stato attuale dell'esperienza dell'utente finale. Ad esempio, se l'esperienza dell'utente è compromessa o parti dell'applicazione non sono attualmente disponibili, fornire tali informazioni.

- Per sospetti attacchi DDoS: se la disponibilità o le prestazioni dell'applicazione sono attualmente compromesse da un possibile attacco DDoS, scegli le seguenti opzioni di gravità e contatto:
  - Per quanto riguarda la gravità, scegli la gravità più alta disponibile per il tuo piano di supporto:
    - Per il supporto aziendale, si tratta di un sistema di produzione inattivo: < 1 ora.
    - Per il supporto Enterprise, si tratta di un sistema business-critical inattivo: < 15 minuti.
  - Per l'opzione di contatto, seleziona Telefono o Chat e fornisci i tuoi dati. L'utilizzo di un metodo di contatto dal vivo fornisce la risposta più rapida.

Coinvolgimento proattivo

Con un coinvolgimento AWS Shield Advanced proattivo, SRT ti contatta direttamente se il controllo dello stato di Amazon Route 53 associato alla tua risorsa protetta non funziona correttamente durante un evento rilevato. Per ulteriori informazioni su questa opzione, consulta Configurazione del coinvolgimento proattivo.

Configurazione di mitigazioni personalizzate con lo Shield Response Team (SRT)

Per i tuoi IP elastici (EIP) e i tuoi acceleratori AWS Global Accelerator standard, puoi collaborare con lo Shield Response Team (SRT) per configurare mitigazioni personalizzate. Ciò è utile nel caso in cui si conosca una logica specifica da applicare quando viene applicata una mitigazione. Ad esempio, potresti voler consentire solo il traffico proveniente da determinati paesi, imporre limiti di velocità specifici, configurare convalide opzionali, non consentire frammenti o consentire solo il traffico che corrisponde a uno schema specifico nel payload dei pacchetti.

Di seguito sono riportati alcuni esempi di mitigazioni personalizzate comuni:

- Pattern matching: se gestisci un servizio che interagisce con applicazioni lato client, puoi scegliere di eseguire la corrispondenza su modelli noti che sono unici per tali applicazioni. Ad esempio, puoi gestire un servizio di gioco o di comunicazione che richiede all'utente finale l'installazione di un software specifico che distribuisci. Puoi includere un numero magico in ogni pacchetto inviato dall'applicazione al tuo servizio. È possibile eseguire la corrispondenza su un massimo di 128 byte (separati o contigui) di un payload e delle intestazioni di un pacchetto TCP o UDP non frammentati. La corrispondenza può essere espressa in notazione esadecimale come offset specifico dall'inizio del payload del pacchetto o offset dinamico dopo un valore noto. Ad esempio, la mitigazione può cercare il byte e quindi aspettarsi i quattro byte `0x01` successivi. `0x12345678`
- DNS specifico: se gestisci il tuo servizio DNS autoritativo utilizzando servizi come Global Accelerator o Amazon Elastic Compute Cloud (Amazon EC2), puoi richiedere una mitigazione personalizzata che convalida i pacchetti per garantire che siano query DNS valide e applicare un punteggio di sospetto che valuti gli attributi specifici del traffico DNS.

Per informazioni su come lavorare con SRT per creare mitigazioni personalizzate, crea un caso di supporto sotto. AWS Shield Per ulteriori informazioni sulla creazione di AWS Support casi, consulta Guida introduttiva. AWS Support

Protezione delle risorse in AWS Shield Advanced

Puoi aggiungere e configurare AWS Shield Advanced protezioni per le tue risorse. È possibile gestire le protezioni per una singola risorsa e raggruppare le risorse protette in raccolte logiche per una migliore gestione degli eventi. Puoi anche tenere traccia delle modifiche alle tue protezioni Shield Advanced utilizzando AWS Config.

Argomenti

AWS Shield Advanced protezioni per tipo di risorsa

Shield Advanced protegge AWS le risorse a livello di rete e trasporto (livelli 3 e 4) e a livello di applicazione (livello 7). È possibile proteggere alcune risorse direttamente e altre tramite l'associazione con risorse protette. Shield Advanced supporta IPv4 e non supporta IPv6.

Questa sezione fornisce informazioni sulle protezioni Shield Advanced per ogni tipo di risorsa.

> **Note**
>
> Shield Advanced protegge solo le risorse specificate in Shield Advanced o tramite una politica AWS Firewall Manager Shield Advanced. Non protegge automaticamente le risorse.

È possibile utilizzare Shield Advanced per il monitoraggio e la protezione avanzati con i seguenti tipi di risorse:

- CloudFront Distribuzioni Amazon. Per la distribuzione CloudFront continua, Shield Advanced protegge qualsiasi distribuzione temporanea associata a una distribuzione primaria protetta.
- Zone ospitate Amazon Route 53.
- AWS Global Accelerator acceleratori standard.
- Indirizzi IP elastici di Amazon EC2. Shield Advanced protegge le risorse associate agli indirizzi IP elastici protetti.
- Istanze Amazon EC2, tramite associazione a indirizzi IP elastici di Amazon EC2.
- I seguenti sistemi di bilanciamento del carico Elastic Load Balancing (ELB):
  - Application Load Balancer.
  - Classic Load Balancer.

- Network Load Balancer, tramite associazioni agli indirizzi IP elastici di Amazon EC2.

Non puoi usare Shield Advanced per proteggere nessun altro tipo di risorsa. Ad esempio, non puoi proteggere gli acceleratori di routing AWS Global Accelerator personalizzati o i Gateway Load Balancer.

È possibile monitorare e proteggere fino a 1.000 risorse per ogni tipo di risorsa. Account AWS Ad esempio, in un singolo account, puoi proteggere 1.000 indirizzi IP elastici di Amazon EC2, 1.000 CloudFront distribuzioni e 1.000 Application Load Balancer. Puoi richiedere un aumento del numero di risorse che puoi proteggere con Shield Advanced tramite la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/.

Protezione delle istanze Amazon EC2 e dei Network Load Balancer con Shield Advanced

Puoi proteggere le istanze Amazon EC2 e i Network Load Balancer collegando prima queste risorse agli indirizzi IP elastici e quindi proteggendo gli indirizzi IP elastici in Shield Advanced.

Quando proteggi gli indirizzi IP elastici, Shield Advanced identifica e protegge le risorse a cui sono collegati. Shield Advanced identifica automaticamente il tipo di risorsa collegata a un indirizzo IP elastico e applica i rilevamenti e le mitigazioni appropriati per tale risorsa. Ciò include la configurazione degli ACL di rete specifici per l'indirizzo IP elastico. Per ulteriori informazioni sull'utilizzo degli indirizzi IP elastici con AWS le tue risorse, consulta le seguenti guide: documentazione di Amazon Elastic Compute Cloud o documentazione Elastic Load Balancing.

Durante un attacco, Shield Advanced distribuisce automaticamente gli ACL di rete ai confini della AWS rete. Quando gli ACL di rete si trovano ai margini della rete, Shield Advanced può fornire protezione da eventi DDoS di grandi dimensioni. In genere, gli ACL di rete vengono applicati vicino alle istanze Amazon EC2 all'interno di Amazon VPC. L'ACL di rete può mitigare gli attacchi solo se il tuo Amazon VPC e la tua istanza sono in grado di gestire. Ad esempio, se l'interfaccia di rete collegata all'istanza Amazon EC2 può elaborare fino a 10 Gbps, i volumi superiori a 10 Gbps rallenteranno e potrebbero bloccare il traffico verso quell'istanza. Durante un attacco, Shield Advanced promuove l'ACL di rete fino al AWS confine, che può elaborare più terabyte di traffico. La lista di controllo degli accessi di rete è in grado di fornire protezione per le risorse ben oltre la capacità tipica della rete. Per ulteriori informazioni sulle liste di controllo degli accessi di rete, consulta l'articolo relativo alle liste di controllo degli accessi di rete.

Alcuni strumenti di scalabilità, ad esempio AWS Elastic Beanstalk, non consentono di collegare automaticamente un indirizzo IP elastico a un Network Load Balancer. In questi casi, è necessario collegare manualmente l'indirizzo IP elastico.

AWS Shield Advanced protezioni a livello di applicazione (livello 7)

Per proteggere le risorse del livello applicativo con Shield Advanced, si inizia associando un ACL AWS WAF Web alla risorsa e aggiungendovi una o più regole basate sulla frequenza. È inoltre possibile abilitare la mitigazione automatica degli attacchi DDoS a livello di applicazione, che consente a Shield Advanced di creare e gestire automaticamente le regole ACL Web per conto dell'utente in risposta agli attacchi DDoS.

Quando proteggi una risorsa a livello di applicazione con Shield Advanced, Shield Advanced analizza il traffico nel tempo per stabilire e mantenere linee di base. Shield Advanced utilizza queste linee di base per rilevare anomalie nei modelli di traffico che potrebbero indicare un attacco DDoS. Il punto in cui Shield Advanced rileva un attacco dipende dal traffico che Shield Advanced è stato in grado di osservare prima dell'attacco e dall'architettura utilizzata per le applicazioni Web. Le variazioni dell'architettura che possono influire sul comportamento di Shield Advanced includono il tipo di istanza utilizzata, la dimensione dell'istanza e se il tipo di istanza supporta reti avanzate. Puoi anche configurare Shield Advanced per implementare automaticamente le mitigazioni per gli attacchi a livello di applicazione.

Abbonamenti e AWS WAF costi Shield Advanced

L'abbonamento a Shield Advanced copre i costi di utilizzo delle AWS WAF funzionalità standard per le risorse protette con Shield Advanced. AWS WAF Le tariffe standard coperte dalle protezioni Shield Advanced sono il costo per ACL Web, il costo per regola e il prezzo base per milione di richieste per l'ispezione delle richieste Web, fino a 1.500 WCU e fino alla dimensione corporea predefinita.

L'attivazione della mitigazione automatica degli attacchi DDoS a livello di applicazione Shield Advanced aggiunge un gruppo di regole all'ACL Web che utilizza 150 unità di capacità ACL Web (WCU). Queste WCU influiscono sull'utilizzo della WCU nell'ACL web. Per ulteriori informazioni, consulta Mitigazione DDoS automatica a livello di applicazione Shield Advanced, Il gruppo di regole Shield Advanced e AWS WAF unità di capacità Web ACL (WCU).

L'abbonamento a Shield Advanced non copre l'uso AWS WAF di risorse che non proteggi utilizzando Shield Advanced. Inoltre, non copre eventuali AWS WAF costi aggiuntivi non standard per le risorse protette. Esempi di AWS WAF costi non standard sono quelli per Bot Control, per l'azione delle CAPTCHA regole, per gli ACL Web che utilizzano più di 1.500 WCU e per l'ispezione del corpo della richiesta oltre le dimensioni corporee predefinite. L'elenco completo è disponibile nella pagina dei prezzi. AWS WAF

Per informazioni complete ed esempi di prezzi, consulta la pagina Prezzi e AWS WAF prezzi di Shield.

Argomenti

- Rilevamento e mitigazione
- ACL AWS WAF Web Shield Advanced a livello applicativo e regole basate sulla velocità
- Mitigazione DDoS automatica a livello di applicazione Shield Advanced

Rilevamento e mitigazione

Questa sezione descrive i fattori che influenzano il rilevamento e la mitigazione degli eventi a livello di applicazione da parte di Shield Advanced.

Controlli dell'integrità

I controlli di integrità che riportano in modo accurato lo stato generale dell'applicazione forniscono a Shield Advanced informazioni sulle condizioni del traffico riscontrate dall'applicazione. Shield Advanced richiede meno informazioni che indicano un potenziale attacco quando l'applicazione segnala un malfunzionamento e richiede più prove di un attacco se l'applicazione lo segnala.

È importante configurare i controlli di integrità in modo che riportino con precisione lo stato delle applicazioni. Per ulteriori informazioni e indicazioni, vedereRilevamento basato sulla salute mediante controlli sanitari.

Linee di base del traffico

Le linee di base sul traffico forniscono a Shield Advanced informazioni sulle caratteristiche del traffico normale per l'applicazione. Shield Advanced utilizza queste linee di base per riconoscere quando l'applicazione non riceve traffico normale, in modo da poterti avvisare e, come configurato, iniziare a ideare e testare opzioni di mitigazione per contrastare un potenziale attacco. Per ulteriori informazioni su come Shield Advanced utilizza le linee di base del traffico per rilevare potenziali eventi, consulta la sezione panoramica. Logica di rilevamento per le minacce a livello di applicazione

Shield Advanced crea le proprie linee di base a partire dalle informazioni fornite dall'ACL Web associata alla risorsa protetta. L'ACL Web deve essere associato alla risorsa per almeno 24 ore e fino a 30 giorni prima che Shield Advanced possa determinare in modo affidabile le linee di base dell'applicazione. Il tempo necessario inizia quando si associa l'ACL Web, tramite Shield Advanced o tramite AWS WAF.

Per ulteriori informazioni sull'utilizzo di un ACL Web con le protezioni a livello di applicazione Shield Advanced, vedere. ACL AWS WAF Web Shield Advanced a livello applicativo e regole basate sulla velocità

Regole basata sulla frequenza

Le regole basate sulla frequenza possono aiutare a mitigare gli attacchi. Inoltre, possono oscurare gli attacchi, mitigandoli prima che diventino un problema abbastanza grande da comparire nelle normali linee di base del traffico o nei report sullo stato dei controlli sanitari.

Ti consigliamo di utilizzare regole basate sulla frequenza nell'ACL Web quando proteggi una risorsa applicativa con Shield Advanced. Anche se le loro mitigazioni possono nascondere un potenziale attacco, sono una preziosa prima linea di difesa, che aiuta a garantire che l'applicazione rimanga disponibile per i clienti legittimi. Il traffico rilevato dalle regole basate sulle tariffe e sul limite di velocità è visibile nelle metriche. AWS WAF

Oltre alle tue regole basate sulla frequenza, se abiliti la mitigazione automatica degli attacchi DDoS a livello di applicazione, Shield Advanced aggiunge un gruppo di regole all'ACL Web che utilizza per mitigare gli attacchi. In questo gruppo di regole, Shield Advanced utilizza sempre una regola basata sulla frequenza che limita il volume di richieste provenienti da indirizzi IP noti per essere fonti di attacchi DDoS. Le metriche per il traffico mitigato dalle regole Shield Advanced non sono disponibili per la visualizzazione.

Per ulteriori informazioni sulle regole basate sulla tariffa, consulta. Istruzione regola basata sulla frequenza Per informazioni sulla regola basata sulla frequenza utilizzata da Shield Advanced per la mitigazione automatica degli attacchi DDoS a livello di applicazione, vedere. Il gruppo di regole Shield Advanced

Per ulteriori informazioni su Shield Advanced e sulle AWS WAF metriche, consultaMonitoraggio con Amazon CloudWatch.

ACL AWS WAF Web Shield Advanced a livello applicativo e regole basate sulla velocità

Per proteggere una risorsa a livello di applicazione con Shield Advanced, iniziate associando un ACL AWS WAF Web alla risorsa. AWS WAF è un firewall per applicazioni Web che consente di monitorare le richieste HTTP e HTTPS inoltrate alle risorse del livello applicativo e consente di controllare l'accesso ai contenuti in base alle caratteristiche delle richieste. È possibile configurare un ACL Web per monitorare e gestire le richieste in base a fattori quali l'origine della richiesta, il

contenuto delle stringhe di query e dei cookie e la frequenza delle richieste provenienti da un singolo indirizzo IP. Come minimo, la protezione Shield Advanced richiede l'associazione di un ACL web a una regola basata sulla velocità, che limita la frequenza delle richieste per ogni indirizzo IP.

Se l'ACL Web associato non ha una regola basata sulla velocità definita, Shield Advanced richiede di definirne almeno una. Le regole basate sulla tariffa bloccano automaticamente il traffico proveniente dagli IP di origine quando superano le soglie definite. Aiutano a proteggere l'applicazione dai flussi di richieste Web e possono fornire avvisi in caso di picchi improvvisi di traffico che potrebbero indicare un potenziale attacco DDoS.

> **Note**
>
> Una regola basata sulla frequenza risponde molto rapidamente ai picchi del traffico monitorato dalla regola. Per questo motivo, una regola basata sulla frequenza può prevenire non solo un attacco, ma anche il rilevamento di un potenziale attacco tramite Shield Advanced detection. Questo compromesso favorisce la prevenzione rispetto alla completa visibilità dei modelli di attacco. Ti consigliamo di utilizzare una regola basata sulla frequenza come prima linea di difesa contro gli attacchi.

Una volta installato l'ACL Web, se si verifica un attacco DDoS, è possibile applicare le mitigazioni aggiungendo e gestendo regole nell'ACL Web. Puoi farlo direttamente, con l'assistenza dello Shield Response Team (SRT), o automaticamente tramite la mitigazione automatica degli attacchi DDoS a livello di applicazione.

> **Important**
>
> Se utilizzi anche la mitigazione automatica degli attacchi DDoS a livello di applicazione, consulta le best practice per la gestione dell'ACL web all'indirizzo. Le migliori pratiche per l'utilizzo della mitigazione automatica

Comportamento predefinito delle regole basate sulla frequenza

Quando si utilizza una regola basata sulla tariffa con la relativa configurazione predefinita, valuta AWS WAF periodicamente il traffico per la finestra temporale precedente di 5 minuti. AWS WAF blocca le richieste provenienti da qualsiasi indirizzo IP che superi la soglia della regola fino a quando la frequenza delle richieste non scende a un livello accettabile. Quando configuri una regola basata

sulla tariffa tramite Shield Advanced, configura la relativa soglia di velocità su un valore superiore alla normale velocità di traffico che ti aspetti da qualsiasi IP di origine in qualsiasi finestra temporale di cinque minuti.

Potresti voler utilizzare più di una regola basata sulla tariffa in un ACL web. Ad esempio, potresti avere una regola basata sulla tariffa per tutto il traffico con una soglia alta più una o più regole aggiuntive configurate per corrispondere a determinate parti dell'applicazione Web e con soglie inferiori. Ad esempio, è possibile associare all'URI `/login.html` una soglia inferiore, per mitigare gli abusi nei confronti di una pagina di accesso.

Puoi configurare una regola basata sulla frequenza per utilizzare una finestra temporale di valutazione diversa e aggregare le richieste in base a una serie di componenti della richiesta, come valori di intestazione, etichette e argomenti di query. Per ulteriori informazioni, consulta Istruzione regola basata sulla frequenza.

Per ulteriori informazioni e indicazioni, consulta il post sul blog sulla sicurezza Le tre regole più importanti basate sulla frequenza. AWS WAF

Opzioni di configurazione estese tramite AWS WAF

La console Shield Advanced consente di aggiungere una regola basata sulla tariffa e configurarla con le impostazioni di base predefinite. È possibile definire opzioni di configurazione aggiuntive gestendo le regole basate sulla tariffa tramite. AWS WAF Ad esempio, puoi configurare la regola per aggregare le richieste in base a chiavi come un indirizzo IP inoltrato, una stringa di query e un'etichetta. Puoi anche aggiungere un'istruzione scope-down alla regola per escludere alcune richieste dalla valutazione e dalla limitazione della velocità. Per ulteriori informazioni, consulta Istruzione regola basata sulla frequenza. Per informazioni sull'utilizzo per AWS WAF gestire le regole di monitoraggio e gestione delle richieste Web, consulta. Creazione di un'ACL Web

Mitigazione DDoS automatica a livello di applicazione Shield Advanced

È possibile configurare Shield Advanced in modo che risponda automaticamente per mitigare gli attacchi a livello di applicazione (livello 7) contro le risorse protette del livello applicativo, contando o bloccando le richieste Web che fanno parte dell'attacco. Questa opzione è un'aggiunta alla protezione a livello di applicazione aggiunta tramite Shield Advanced con un ACL AWS WAF Web e una regola basata sulla tariffa personalizzata.

Quando la mitigazione automatica è abilitata per una risorsa, Shield Advanced mantiene un gruppo di regole nell'ACL web associato alla risorsa dove gestisce le regole di mitigazione per conto della

risorsa. Il gruppo di regole contiene una regola basata sulla frequenza che tiene traccia del volume di richieste provenienti da indirizzi IP noti per essere fonti di attacchi DDoS.

Inoltre, Shield Advanced confronta i modelli di traffico attuali con le linee di base del traffico storico per rilevare deviazioni che potrebbero indicare un attacco DDoS. Shield Advanced risponde agli attacchi DDoS rilevati creando, valutando e implementando AWS WAF regole personalizzate aggiuntive nel gruppo di regole.

Indice

Avvertenze per l'utilizzo della mitigazione automatica

L'elenco seguente descrive gli avvertimenti della mitigazione automatica degli attacchi DDoS a livello di applicazione Shield Advanced e descrive i passaggi che potresti voler intraprendere in risposta.

- La mitigazione automatica degli attacchi DDoS a livello di applicazione funziona solo con gli ACL Web creati utilizzando l'ultima versione di (v2). AWS WAF
- Shield Advanced richiede tempo per stabilire una base del traffico normale e storico dell'applicazione, che sfrutta per rilevare e isolare il traffico di attacco dal traffico normale e mitigare il traffico di attacco. Il tempo necessario per stabilire una linea di base è compreso tra 24 ore e 30 giorni dal momento in cui si associa un ACL Web alla risorsa applicativa protetta. Per ulteriori informazioni sulle linee di base del traffico, vedere. Rilevamento e mitigazione
- L'attivazione della mitigazione automatica degli attacchi DDoS a livello di applicazione aggiunge un gruppo di regole all'ACL Web che utilizza 150 unità di capacità ACL Web (WCU). Queste WCU influiscono sull'utilizzo della WCU nell'ACL web. Per ulteriori informazioni, consulta Il gruppo di regole Shield Advanced e AWS WAF unità di capacità Web ACL (WCU).
- Il gruppo di regole Shield Advanced genera AWS WAF metriche, ma non sono disponibili per la visualizzazione. È lo stesso di qualsiasi altro gruppo di regole che utilizzi nell'ACL Web ma che non possiedi, come i gruppi di regole AWS Managed Rules. Per ulteriori informazioni sulle AWS WAF metriche, consulta. AWS WAF metriche e dimensioni Per informazioni su questa opzione di protezione Shield Advanced, vedereMitigazione DDoS automatica a livello di applicazione Shield Advanced.
- Per gli ACL Web che proteggono più risorse, la mitigazione automatica implementa solo mitigazioni personalizzate che non hanno un impatto negativo su nessuna delle risorse protette.
- Il tempo che intercorre tra l'inizio di un attacco DDoS e il momento in cui Shield Advanced imposta regole di mitigazione automatiche personalizzate varia a seconda dell'evento. Alcuni attacchi DDoS potrebbero terminare prima dell'implementazione delle regole personalizzate. Altri attacchi potrebbero verificarsi quando è già in atto una mitigazione e quindi potrebbero essere mitigati da tali regole sin dall'inizio dell'evento. Inoltre, le regole basate sulla frequenza nel gruppo di regole Web ACL e Shield Advanced potrebbero mitigare il traffico di attacco prima che venga rilevato come un possibile evento.
- Per gli Application Load Balancer che ricevono traffico attraverso una rete di distribuzione dei contenuti (CDN), come Amazon CloudFront, le funzionalità di mitigazione automatica a livello di applicazione di Shield Advanced per tali risorse di Application Load Balancer saranno ridotte. Shield Advanced utilizza gli attributi del traffico client per identificare e isolare il traffico di attacco dal traffico normale verso l'applicazione e le CDN potrebbero non conservare o inoltrare gli attributi originali del traffico client. Se lo utilizzi CloudFront, ti consigliamo di abilitare la mitigazione automatica sulla distribuzione. CloudFront
- La mitigazione automatica degli attacchi DDoS a livello di applicazione non interagisce con i gruppi di protezione. È possibile abilitare la mitigazione automatica per le risorse che si trovano nei gruppi

di protezione, ma Shield Advanced non applica automaticamente le mitigazioni degli attacchi in base ai risultati dei gruppi di protezione. Shield Advanced applica mitigazioni automatiche degli attacchi per le singole risorse.

Le migliori pratiche per l'utilizzo della mitigazione automatica

Attenetevi alle indicazioni fornite in questa sezione quando utilizzate la mitigazione automatica.

Gestione generale delle protezioni

Segui queste linee guida per pianificare e implementare le protezioni automatiche di mitigazione.

- Gestisci tutte le tue protezioni automatiche di mitigazione tramite Shield Advanced o, se utilizzi AWS Firewall Manager per gestire le impostazioni di mitigazione automatica Shield Advanced, tramite Firewall Manager. Non mischiate l'uso di Shield Advanced e Firewall Manager per gestire queste protezioni.
- Gestisci risorse simili utilizzando gli stessi ACL Web e le stesse impostazioni di protezione e gestisci risorse diverse utilizzando ACL Web diversi. Quando Shield Advanced mitiga un attacco DDoS su una risorsa protetta, definisce le regole per l'ACL Web associato alla risorsa e quindi verifica le regole rispetto al traffico di tutte le risorse associate all'ACL Web. Shield Advanced applicherà le regole solo se non hanno un impatto negativo su nessuna delle risorse associate. Per ulteriori informazioni, consulta Come Shield Advanced gestisce la mitigazione automatica.
- Per gli Application Load Balancer che hanno tutto il traffico Internet inoltrato tramite proxy tramite una CloudFront distribuzione Amazon, abilita solo la mitigazione automatica sulla distribuzione. CloudFront La CloudFront distribuzione avrà sempre il maggior numero di attributi di traffico originali, che Shield Advanced sfrutta per mitigare gli attacchi.

Ottimizzazione del rilevamento e della mitigazione

Segui queste linee guida per ottimizzare le protezioni che la mitigazione automatica fornisce alle risorse protette. Per una panoramica del rilevamento e della mitigazione a livello di applicazione, vedere. Rilevamento e mitigazione

- Configura i controlli di integrità per le tue risorse protette e usali per abilitare il rilevamento basato sullo stato nelle tue protezioni Shield Advanced. Per le linee guida, consulta Rilevamento basato sulla salute mediante controlli sanitari.

- Abilita la mitigazione automatica in Count modalità fino a quando Shield Advanced non ha stabilito una linea di base per il traffico normale e storico. Shield Advanced richiede da 24 ore a 30 giorni per stabilire una linea di base.

  La definizione di una linea di base dei normali modelli di traffico richiede quanto segue:

  - L'associazione di un ACL web con la risorsa protetta. È possibile utilizzare AWS WAF direttamente per associare l'ACL Web oppure fare in modo che Shield Advanced lo associ quando si abilita la protezione a livello di applicazione Shield Advanced e si specifica un ACL Web da utilizzare.
  - Flusso di traffico normale verso l'applicazione protetta. Se l'applicazione non riceve traffico normale, ad esempio prima del lancio dell'applicazione o se manca traffico di produzione per lunghi periodi di tempo, i dati storici non possono essere raccolti.

Gestione Web ACL

Segui queste linee guida per la gestione degli ACL Web che utilizzi con la mitigazione automatica.

- Se devi sostituire l'ACL web associato alla risorsa protetta, apporta le seguenti modifiche nell'ordine:

  1. In Shield Advanced, disabilita la mitigazione automatica.
  2. In AWS WAF, dissocia il vecchio ACL web e associa il nuovo ACL web.
  3. In Shield Advanced, abilita la mitigazione automatica.

  Shield Advanced non trasferisce automaticamente la mitigazione automatica dal vecchio ACL web a quello nuovo.
- Non eliminate alcuna regola del gruppo di regole dai vostri ACL web il cui nome inizia con. `ShieldMitigationRuleGroup` Se elimini questo gruppo di regole, disabiliti le protezioni fornite dalla mitigazione automatica Shield Advanced per ogni risorsa associata all'ACL web. Inoltre, Shield Advanced potrebbe impiegare del tempo per ricevere la notifica della modifica e aggiornare le impostazioni. Durante questo periodo, le pagine della console Shield Advanced forniranno informazioni errate.

  Per ulteriori informazioni sul gruppo di regole, vedereIl gruppo di regole Shield Advanced.
- Non modificare il nome di una regola del gruppo di regole il cui nome inizia con`ShieldMitigationRuleGroup`. Ciò può interferire con le protezioni fornite dalla mitigazione automatica Shield Advanced tramite l'ACL web.

- Quando crei regole e gruppi di regole, non utilizzare nomi che iniziano con. `ShieldMitigationRuleGroup` Questa stringa viene utilizzata da Shield Advanced per gestire le mitigazioni automatiche.
- Nella gestione delle regole ACL Web, non assegnate un'impostazione di priorità di 10.000.000. Shield Advanced assegna questa impostazione di priorità alla regola del gruppo di regole di mitigazione automatica quando la aggiunge.
- Mantieni la `ShieldMitigationRuleGroup` regola prioritaria in modo che venga eseguita quando vuoi rispetto alle altre regole del tuo ACL web. Shield Advanced aggiunge la regola del gruppo di regole all'ACL Web con priorità 10.000.000, da eseguire dopo le altre regole. Se utilizzi la procedura guidata della AWS WAF console per gestire l'ACL Web, modifica le impostazioni di priorità in base alle esigenze dopo aver aggiunto le regole all'ACL Web.
- Se utilizzi AWS CloudFormation per gestire gli ACL Web, non è necessario gestire la regola del `ShieldMitigationRuleGroup` gruppo di regole. Segui le istruzioni riportate all'Utilizzo AWS CloudFormation con mitigazione automatica degli attacchi DDoS a livello di applicazioneindirizzo.

Configurazione richiesta per abilitare la mitigazione automatica

Abilita la mitigazione automatica Shield Advanced come parte delle protezioni DDoS a livello di applicazione per la tua risorsa. Per informazioni su come eseguire questa operazione tramite la console, consulta. Configura le protezioni DDoS a livello di applicazione

La funzionalità di mitigazione automatica richiede le seguenti operazioni:

- Associa un ACL Web alla risorsa: è necessario per qualsiasi protezione a livello di applicazione Shield Advanced. È possibile utilizzare lo stesso ACL Web per più risorse. Ti consigliamo di eseguire questa operazione solo per risorse con traffico simile. Per informazioni sugli ACL Web, inclusi i requisiti per utilizzarli con più risorse, consultaCome AWS WAF funziona.
- Abilita e configura la mitigazione automatica degli attacchi DDoS a livello di applicazione Shield Advanced: abilitando questa opzione, specifichi se desideri che Shield Advanced blocchi o conti automaticamente le richieste Web che ritiene facciano parte di un attacco DDoS. Shield Advanced aggiunge un gruppo di regole all'ACL Web associato e lo utilizza per gestire dinamicamente la risposta agli attacchi DDoS alla risorsa. Per informazioni sulle opzioni di azione delle regole, consulta. Operazione delle regole
- (Facoltativo, ma consigliato) Aggiungi una regola basata sulla frequenza all'ACL Web: per impostazione predefinita, la regola basata sulla frequenza fornisce alla risorsa una protezione di base contro gli attacchi DDoS impedendo a un singolo indirizzo IP di inviare troppe richieste

in breve tempo. Per informazioni sulle regole basate sulla tariffa, incluse opzioni ed esempi di aggregazione delle richieste personalizzate, consulta. Istruzione regola basata sulla frequenza

Come Shield Advanced gestisce la mitigazione automatica

Gli argomenti della sezione descrivono come Shield Advanced gestisce le modifiche alla configurazione per la mitigazione automatica degli attacchi DDoS a livello di applicazione e come gestisce gli attacchi DDoS quando la mitigazione automatica è abilitata.

Argomenti

- Cosa succede quando si abilita la mitigazione automatica
- In che modo Shield Advanced risponde agli attacchi DDoS con la mitigazione automatica
- In che modo Shield Advanced gestisce l'impostazione delle azioni delle regole
- In che modo Shield Advanced gestisce le mitigazioni quando un attacco si attenua
- Cosa succede quando si disabilita la mitigazione automatica

Cosa succede quando si abilita la mitigazione automatica

Shield Advanced esegue le seguenti operazioni quando si abilita la mitigazione automatica:

- Se necessario, aggiunge un gruppo di regole per l'uso di Shield Advanced: se l'ACL AWS WAF Web associato alla risorsa non dispone già di una AWS WAF regola del gruppo di regole dedicata alla mitigazione automatica degli attacchi DDoS a livello di applicazione, Shield Advanced ne aggiunge una.

  Il nome della regola del gruppo di regole inizia con. `ShieldMitigationRuleGroup` Il gruppo di regole contiene sempre una regola basata sulla frequenza denominata`ShieldKnownOffenderIPRateBasedRule`, che limita il volume di richieste provenienti da indirizzi IP noti per essere fonti di attacchi DDoS. Per ulteriori dettagli sul gruppo di regole Shield Advanced e sulla regola Web ACL che vi fa riferimento, vedereIl gruppo di regole Shield Advanced.
- Inizia a rispondere agli attacchi DDoS contro la risorsa: Shield Advanced risponde automaticamente agli attacchi DDoS per la risorsa protetta. Oltre alla regola basata sulla frequenza, che è sempre presente, Shield Advanced utilizza il proprio gruppo di regole per implementare AWS WAF regole personalizzate per la mitigazione degli attacchi DDoS. Shield Advanced adatta queste regole alla tua applicazione e agli attacchi che subisce la tua applicazione e le testa rispetto al traffico storico della risorsa prima di implementarle.

Shield Advanced utilizza una singola regola del gruppo di regole in qualsiasi ACL Web utilizzato per la mitigazione automatica. Se Shield Advanced ha già aggiunto il gruppo di regole per un'altra risorsa protetta, non aggiunge un altro gruppo di regole all'ACL Web.

La mitigazione automatica degli attacchi DDoS a livello di applicazione dipende dalla presenza del gruppo di regole per mitigare gli attacchi. Se il gruppo di regole viene rimosso dall'ACL AWS WAF Web per qualsiasi motivo, la rimozione disabilita la mitigazione automatica per tutte le risorse associate all'ACL Web.

In che modo Shield Advanced risponde agli attacchi DDoS con la mitigazione automatica

Quando la mitigazione automatica è abilitata su una risorsa protetta, la regola `ShieldKnownOffenderIPRateBasedRule` basata sulla tariffa nel gruppo di regole Shield Advanced risponde automaticamente ai volumi di traffico elevati provenienti da fonti DDoS note. Questa limitazione della velocità viene applicata rapidamente e funge da difesa in prima linea contro gli attacchi.

Quando Shield Advanced rileva un attacco, esegue le seguenti operazioni:

1. Tenta di identificare una firma di attacco che isola il traffico di attacco dal normale traffico verso l'applicazione. L'obiettivo è produrre regole di mitigazione degli attacchi DDoS di alta qualità che, se applicate, influiscano solo sul traffico di attacco e non influiscano sul normale traffico verso l'applicazione.
2. Valuta la firma dell'attacco identificata rispetto ai modelli di traffico storici per la risorsa sotto attacco e per qualsiasi altra risorsa associata allo stesso ACL web. Shield Advanced esegue questa operazione prima di implementare qualsiasi regola in risposta all'evento.

   A seconda dei risultati della valutazione, Shield Advanced esegue una delle seguenti operazioni:

   - Se Shield Advanced determina che la firma di attacco isola solo il traffico coinvolto nell'attacco DDoS, implementa la firma nelle AWS WAF regole del gruppo di regole di mitigazione Shield Advanced nell'ACL web. Shield Advanced fornisce a queste regole l'impostazione di azione che hai configurato per la mitigazione automatica della risorsa, Count oppureBlock.
   - Altrimenti, Shield Advanced non prevede alcuna mitigazione.

Durante un attacco, Shield Advanced invia le stesse notifiche e fornisce le stesse informazioni sugli eventi delle protezioni di base a livello di applicazione Shield Advanced. Puoi visualizzare le informazioni sugli eventi e sugli attacchi DDoS e su qualsiasi mitigazione degli attacchi Shield

Advanced nella console degli eventi Shield Advanced. Per informazioni, consulta Visibilità sugli eventi DDoS.

Se hai configurato la mitigazione automatica per utilizzare l'azione della Block regola e riscontri falsi positivi nelle regole di mitigazione implementate da Shield Advanced, puoi modificare l'azione della regola in. Count Per informazioni su come eseguire questa operazione, consulta. Modifica dell'azione utilizzata per la mitigazione automatica degli attacchi DDoS a livello di applicazione

In che modo Shield Advanced gestisce l'impostazione delle azioni delle regole

Puoi impostare l'azione della regola per le tue mitigazioni automatiche su Block o. Count

Quando si modifica l'impostazione dell'azione automatica delle regole di mitigazione per una risorsa protetta, Shield Advanced aggiorna tutte le impostazioni delle regole per la risorsa. Aggiorna tutte le regole attualmente in vigore per la risorsa nel gruppo di regole Shield Advanced e utilizza la nuova impostazione di azione quando crea nuove regole.

Per le risorse che utilizzano lo stesso ACL Web, se si specificano azioni diverse, Shield Advanced utilizza l'impostazione dell'Blockazione per la regola basata sulla frequenza del gruppo di regole. `ShieldKnownOffenderIPRateBasedRule` Shield Advanced crea e gestisce altre regole nel gruppo di regole per conto di una specifica risorsa protetta e utilizza l'impostazione di azione specificata per la risorsa. Tutte le regole del gruppo di regole Shield Advanced in un ACL Web vengono applicate al traffico Web di tutte le risorse associate.

La propagazione della modifica dell'impostazione dell'azione può richiedere alcuni secondi. Durante questo periodo, potresti vedere la vecchia impostazione in alcuni punti in cui è in uso il gruppo di regole e la nuova impostazione in altri.

È possibile modificare l'impostazione dell'azione delle regole per la configurazione di mitigazione automatica nella pagina degli eventi della console e tramite la pagina di configurazione del livello di applicazione. Per informazioni sulla pagina degli eventi, vedereRisposta agli eventi DDoS. Per informazioni sulla pagina di configurazione, vedereConfigura le protezioni DDoS a livello di applicazione.

In che modo Shield Advanced gestisce le mitigazioni quando un attacco si attenua

Quando Shield Advanced determina che le regole di mitigazione che sono state implementate per un particolare attacco non sono più necessarie, le rimuove dal gruppo di regole di mitigazione Shield Advanced.

La rimozione delle regole di mitigazione non coinciderà necessariamente con la fine di un attacco. Shield Advanced monitora i modelli di attacco che rileva sulle risorse protette. Potrebbe difendersi in modo proattivo dalla recidiva di un attacco con una firma specifica mantenendo in vigore le regole che ha implementato contro il verificarsi iniziale di quell'attacco. Se necessario, Shield Advanced aumenta il lasso di tempo necessario per mantenere le regole in vigore. In questo modo, Shield Advanced potrebbe mitigare gli attacchi ripetuti con una firma specifica prima che abbiano un impatto sulle risorse protette.

Shield Advanced non rimuove mai la regola basata sulla frequenza`ShieldKnownOffenderIPRateBasedRule`, che limita il volume di richieste provenienti da indirizzi IP noti per essere fonti di attacchi DDoS.

Cosa succede quando si disabilita la mitigazione automatica

Shield Advanced esegue le seguenti operazioni quando si disabilita la mitigazione automatica per una risorsa:

- Interrompe la risposta automatica agli attacchi DDoS: Shield Advanced interrompe le attività di risposta automatica per la risorsa.
- Rimuove le regole non necessarie dal gruppo di regole Shield Advanced: se Shield Advanced mantiene delle regole nel proprio gruppo di regole gestito per conto della risorsa protetta, le rimuove.
- Rimuove il gruppo di regole Shield Advanced, se non è più in uso: se l'ACL Web associato alla risorsa non è associato a nessun'altra risorsa con la mitigazione automatica abilitata, Shield Advanced rimuove la regola del gruppo di regole dall'ACL Web.

Il gruppo di regole Shield Advanced

Shield Advanced gestisce le attività di mitigazione automatica utilizzando le regole di un gruppo di regole di cui è proprietario e gestisce per conto dell'utente. Shield Advanced fa riferimento al gruppo di regole con una regola nell'ACL Web associata alla risorsa protetta.

La regola del gruppo di regole nell'ACL web

La regola del gruppo di regole Shield Advanced nell'ACL Web ha le seguenti proprietà:

- Nome: `ShieldMitigationRuleGroup_`*`account-id`*`_`*`web-acl-id`*`_`*`unique-identifier`*
- Unità di capacità Web ACL (WCU): 150. Queste WCU influiscono sull'utilizzo della WCU nell'ACL web.

Shield Advanced crea questa regola nell'ACL Web con un'impostazione di priorità di 10.000.000, in modo che venga eseguita dopo le altre regole e gruppi di regole nell'ACL Web. AWS WAF esegue le regole in un ACL web dall'impostazione di priorità numerica più bassa in poi. Durante la gestione dell'ACL Web, questa impostazione di priorità potrebbe cambiare.

La funzionalità di mitigazione automatica non consuma AWS WAF risorse aggiuntive nel tuo account, a parte le WCU utilizzate dal gruppo di regole nell'ACL web. Ad esempio, il gruppo di regole Shield Advanced non viene conteggiato come uno dei gruppi di regole del tuo account. Per informazioni sui limiti degli account in AWS WAF, consultaAWS WAF quote.

Regole nel gruppo di regole

All'interno del gruppo di regole Shield Advanced di riferimento, Shield Advanced mantiene una regola basata sulla frequenza`ShieldKnownOffenderIPRateBasedRule`, che limita il volume di richieste provenienti da indirizzi IP noti per essere fonti di attacchi DDoS. Questa regola funge da prima linea di difesa contro qualsiasi attacco, perché è sempre presente nel gruppo di regole e non si basa sull'analisi dei modelli di traffico per contenere gli attacchi. L'azione di questa regola è impostata sull'azione scelta per le mitigazioni automatiche, proprio come le altre regole del gruppo di regole. Per informazioni sulle regole basate sulle tariffe, consulta. Istruzione regola basata sulla frequenza

> **Note**
>
> La regola basata sulla frequenza `ShieldKnownOffenderIPRateBasedRule` funziona indipendentemente dal rilevamento degli eventi Shield Advanced. Sebbene la mitigazione automatica sia abilitata, questa regola limita gli indirizzi IP noti per essere fonti di attacchi DDoS. Per questi indirizzi IP, la limitazione della velocità della regola può prevenire gli attacchi e anche impedire che gli attacchi compaiano nelle informazioni di rilevamento di Shield Advanced. Questo compromesso privilegia la prevenzione rispetto alla completa visibilità dei modelli di attacco.

Oltre alla regola permanente basata sulla tariffa descritta sopra, il gruppo di regole contiene tutte le regole attualmente utilizzate da Shield Advanced per mitigare gli attacchi DDoS. Shield Advanced aggiunge, modifica e rimuove queste regole secondo necessità. Per informazioni, consulta Come Shield Advanced gestisce la mitigazione automatica.

Metriche

Il gruppo di regole genera AWS WAF metriche, ma poiché questo gruppo di regole è di proprietà di Shield Advanced, queste metriche non sono disponibili per la visualizzazione. Per ulteriori informazioni, consulta AWS WAF metriche e dimensioni.

Gestione della mitigazione automatica degli attacchi DDoS a livello di applicazione

Utilizza le indicazioni contenute in questa sezione per gestire le configurazioni automatiche di mitigazione degli attacchi DDoS a livello di applicazione. Per informazioni su come funziona la mitigazione automatica, consulta gli argomenti precedenti.

> **Note**
>
> Segui le migliori pratiche descritte in. Le migliori pratiche per l'utilizzo della mitigazione automatica

Argomenti

- Visualizzazione della configurazione automatica di mitigazione degli attacchi DDoS a livello di applicazione per una risorsa
- Abilitazione e disabilitazione della mitigazione automatica degli attacchi DDoS a livello di applicazione
- Modifica dell'azione utilizzata per la mitigazione automatica degli attacchi DDoS a livello di applicazione
- Utilizzo AWS CloudFormation con mitigazione automatica degli attacchi DDoS a livello di applicazione

Visualizzazione della configurazione automatica di mitigazione degli attacchi DDoS a livello di applicazione per una risorsa

È possibile visualizzare la configurazione automatica della mitigazione degli attacchi DDoS a livello di applicazione per una risorsa nella pagina Risorse protette e nelle pagine di protezione individuali.

Per visualizzare la configurazione automatica della mitigazione degli attacchi DDoS a livello di applicazione

1. Accedi AWS Management Console e apri la console AWS WAF & Shield all'indirizzo https://console.aws.amazon.com/wafv2/.

2. Nel pannello AWS Shield di navigazione, scegli Risorse protette. Nell'elenco delle risorse protette, la colonna Attenuazione automatica degli attacchi DDoS a livello di applicazione indica se la mitigazione automatica è abilitata e, se abilitata, l'azione che Shield Advanced deve utilizzare nelle sue mitigazioni.

   Puoi anche selezionare qualsiasi risorsa a livello di applicazione per visualizzare le stesse informazioni elencate nella pagina delle protezioni per la risorsa.

Abilitazione e disabilitazione della mitigazione automatica degli attacchi DDoS a livello di applicazione

La procedura seguente mostra come abilitare o disabilitare la risposta automatica per una risorsa protetta.

Per abilitare o disabilitare la mitigazione automatica degli attacchi DDoS a livello di applicazione per una singola risorsa

1. Accedi AWS Management Console e apri la console AWS WAF & Shield all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel pannello AWS Shield di navigazione, scegli Risorse protette.
3. Nella scheda Protezioni, seleziona la risorsa del livello di applicazione per cui desideri abilitare la mitigazione automatica. Viene visualizzata la pagina delle protezioni per la risorsa.
4. Nella pagina delle protezioni della risorsa, scegli Modifica.
5. Nella pagina Configura la mitigazione DDoS di livello 7 per le risorse globali: facoltativo, per la mitigazione degli attacchi DDoS a livello di applicazione automatica, scegli l'opzione che desideri utilizzare per le mitigazioni automatiche. Le opzioni nella console sono le seguenti:

   - Mantieni le impostazioni correnti: non apportare modifiche alle impostazioni di mitigazione automatica della risorsa protetta.
   - Abilita: abilita la mitigazione automatica per la risorsa protetta. Quando scegli questa opzione, seleziona anche l'azione della regola che desideri che le mitigazioni automatiche utilizzino nelle regole ACL Web. Per informazioni sulle impostazioni delle azioni delle regole, consulta. Operazione delle regole

     Se la risorsa protetta non ha ancora una cronologia del normale traffico applicativo, abilita la mitigazione automatica in Count modalità fino a quando Shield Advanced non sarà in grado di stabilire una linea di base. Shield Advanced inizia a raccogliere informazioni per la sua linea di

base quando si associa un ACL Web alla risorsa protetta e possono essere necessari da 24 ore a 30 giorni per stabilire una buona linea di base del traffico normale.

- Disattiva: disabilita la mitigazione automatica per la risorsa protetta.

6. Scorri il resto delle pagine fino a completare e salvare la configurazione.

Nella pagina Protezioni, le impostazioni di mitigazione automatica vengono aggiornate per la risorsa.

Modifica dell'azione utilizzata per la mitigazione automatica degli attacchi DDoS a livello di applicazione

Puoi modificare l'azione utilizzata da Shield Advanced per la risposta automatica a livello di applicazione in più posizioni della console:

- Configurazione di mitigazione automatica: modifica l'azione quando configuri la mitigazione automatica per la tua risorsa. Per la procedura, vedere la sezione precedente. Abilitazione e disabilitazione della mitigazione automatica degli attacchi DDoS a livello di applicazione
- Pagina dei dettagli dell'evento: modifica l'azione nella pagina dei dettagli dell'evento, quando visualizzi le informazioni sull'evento nella console. Per informazioni, consulta AWS Shield Advanced dettagli dell'evento.

Se si dispone di due risorse protette che condividono un ACL Web e si imposta l'azione su una e Block sull'altra, Shield Advanced imposta l'azione per la regola basata sulla frequenza del gruppo di regole su. Count `ShieldKnownOffenderIPRateBasedRule` Block

Utilizzo AWS CloudFormation con mitigazione automatica degli attacchi DDoS a livello di applicazione

Scopri come utilizzarla per AWS CloudFormation gestire le protezioni e gli ACL web. AWS WAF

Abilitazione o disabilitazione della mitigazione automatica degli attacchi DDoS a livello di applicazione

È possibile abilitare e disabilitare la mitigazione automatica degli attacchi DDoS a livello di applicazione tramite AWS CloudFormation, utilizzando la risorsa. `AWS::Shield::Protection` L'effetto è lo stesso che si ottiene quando si abilita o si disabilita la funzionalità tramite la console o qualsiasi altra interfaccia. Per informazioni sulla AWS CloudFormation risorsa, consulta AWS::Shield::Protectionla guida per l'AWS CloudFormation utente.

Gestione degli ACL Web utilizzati con mitigazione automatica

Shield Advanced gestisce la mitigazione automatica per la risorsa protetta utilizzando una regola del gruppo di regole nell'ACL AWS WAF Web della risorsa protetta. Tramite la AWS WAF console e le API, vedrai la regola elencata nelle tue regole ACL web, con un nome che inizia con. `ShieldMitigationRuleGroup` Questa regola è dedicata alla mitigazione automatica degli attacchi DDoS a livello di applicazione ed è gestita per te da Shield Advanced and. AWS WAF Per ulteriori informazioni, consultare Il gruppo di regole Shield Advanced e Come Shield Advanced gestisce la mitigazione automatica.

Se lo utilizzi AWS CloudFormation per gestire i tuoi ACL Web, non aggiungere la regola del gruppo di regole Shield Advanced al tuo modello ACL Web. Quando aggiorni un ACL web che viene utilizzato con le tue protezioni di mitigazione automatiche, gestisce AWS WAF automaticamente la regola del gruppo di regole nell'ACL web.

Vedrai le seguenti differenze rispetto agli altri ACL web che gestisci tramite: AWS CloudFormation

- AWS CloudFormation non segnalerà alcuna deviazione nello stato di deriva dello stack tra la configurazione effettiva dell'ACL Web, con la regola del gruppo di regole Shield Advanced, e il modello ACL Web, senza la regola. La regola Shield Advanced non verrà visualizzata nell'elenco effettivo della risorsa nei dettagli della deriva.

  Potrai vedere la regola del gruppo di regole Shield Advanced negli elenchi ACL Web da cui richiami AWS WAF, ad esempio tramite la AWS WAF console o AWS WAF le API.
- Se modifichi il modello ACL Web in uno stack e AWS WAF Shield Advanced mantiene automaticamente la regola di mitigazione automatica Shield Advanced nell'ACL Web aggiornato. Le protezioni di mitigazione automatiche fornite da Shield Advanced non vengono interrotte dall'aggiornamento all'ACL Web.

Non gestite la regola Shield Advanced nel vostro modello ACL AWS CloudFormation web. Il modello Web ACL non dovrebbe elencare la regola Shield Advanced. Segui le migliori pratiche per la gestione degli ACL Web all'indirizzo. Le migliori pratiche per l'utilizzo della mitigazione automatica

Rilevamento basato sulla salute mediante controlli sanitari

Puoi configurare Shield Advanced per utilizzare il rilevamento basato sullo stato di salute per migliorare la reattività e la precisione nel rilevamento e nella mitigazione degli attacchi. È possibile utilizzare questa opzione con qualsiasi tipo di risorsa ad eccezione delle zone ospitate su Route 53.

Per configurare il rilevamento basato sullo stato, definisci un controllo dello stato della tua risorsa in Route 53, verifichi che stia segnalando lo stato di salute e quindi associala alla protezione Shield

Advanced. Per informazioni sui controlli di integrità di Route 53, consulta Come Amazon Route 53 verifica lo stato delle tue risorse e Creazione, aggiornamento ed eliminazione dei controlli di integrità nella Amazon Route 53 Developer Guide.

> **Note**
>
> I controlli Health sono necessari per il supporto proattivo al coinvolgimento dello Shield Response Team (SRT). Per informazioni sul coinvolgimento proattivo, consulta. Configurazione del coinvolgimento proattivo

I controlli sanitari misurano lo stato delle risorse in base ai requisiti che definisci. Lo stato del controllo dello stato fornisce un input fondamentale ai meccanismi di rilevamento Shield Advanced, offrendo loro una maggiore sensibilità allo stato attuale delle applicazioni specifiche.

È possibile abilitare il rilevamento basato sullo stato di salute per qualsiasi tipo di risorsa ad eccezione delle zone ospitate da Route 53.

- Risorse a livello di rete e trasporto (livello 3/livello 4): il rilevamento basato sull'integrità migliora la precisione del rilevamento e della mitigazione degli eventi a livello di rete e trasporto per Network Load Balancer, indirizzi IP elastici e acceleratori standard Global Accelerator. Quando proteggi questi tipi di risorse con Shield Advanced, Shield Advanced può fornire mitigazioni per attacchi più piccoli e mitigazioni più rapide per gli attacchi, anche quando il traffico rientra nella capacità dell'applicazione.

  Quando si aggiunge il rilevamento basato sullo stato di salute, durante i periodi in cui il relativo controllo sanitario non è corretto, Shield Advanced può effettuare le mitigazioni ancora più rapidamente e a soglie ancora più basse.
- Risorse a livello applicativo (livello 7): il rilevamento basato sullo stato di salute migliora la precisione del rilevamento dei flussi di richieste Web per CloudFront le distribuzioni e gli Application Load Balancer. Quando proteggi questi tipi di risorse con Shield Advanced, ricevi avvisi di rilevamento delle inondazioni di richieste Web quando si verifica una deviazione statisticamente significativa nel volume di traffico combinata con cambiamenti significativi nei modelli di traffico, in base alle caratteristiche della richiesta.

  Con il rilevamento basato sullo stato di salute, quando il controllo dello stato della Route 53 associato non è integro, Shield Advanced richiede deviazioni minori per avvisare e riporta gli eventi

più rapidamente. Al contrario, quando il controllo dello stato della Route 53 associato è corretto, Shield Advanced richiede deviazioni maggiori per avvisare.

Indice

Le migliori pratiche per l'utilizzo dei controlli sanitari con Shield Advanced

Segui le best practice riportate in questa sezione quando crei e utilizzi i controlli di integrità con Shield Advanced.

- Pianifica i tuoi controlli sanitari identificando i componenti dell'infrastruttura che desideri monitorare. Considerate i seguenti tipi di risorse per i controlli sanitari:
  - Risorse critiche.
  - Qualsiasi risorsa per cui desideri una maggiore sensibilità nel rilevamento e nella mitigazione di Shield Advanced.
  - Risorse per le quali desideri che Shield Advanced ti contatti in modo proattivo. Il coinvolgimento proattivo si basa sullo stato dei controlli sanitari.

  Esempi di risorse che potresti voler monitorare includono le CloudFront distribuzioni Amazon, i sistemi di bilanciamento del carico con connessione a Internet e le istanze Amazon EC2.
- Definisci controlli di integrità che riflettano accuratamente lo stato dell'origine dell'applicazione con il minor numero possibile di notifiche.

- Esegui controlli di integrità in modo che non siano integri solo quando l'applicazione non è disponibile o non funziona entro parametri accettabili. Sei responsabile della definizione e del mantenimento dei controlli di integrità in base ai requisiti specifici dell'applicazione.
- Utilizzate il minor numero possibile di controlli sanitari, pur continuando a riferire in modo accurato sullo stato della vostra applicazione. Ad esempio, allarmi multipli provenienti da più aree dell'applicazione e che segnalano tutti lo stesso problema potrebbero aumentare i costi delle attività di risposta senza aggiungere valore informativo.
- Utilizza controlli di integrità calcolati per monitorare lo stato delle applicazioni utilizzando una combinazione di CloudWatch parametri Amazon. Ad esempio, puoi calcolare l'integrità combinata in base alla latenza dei tuoi server delle applicazioni e al loro tasso di errore di 5xx, il che indica che il server di origine non ha soddisfatto la richiesta.
- Create e pubblicate gli indicatori di integrità delle vostre applicazioni con metriche CloudWatch personalizzate in base alle esigenze e utilizzateli in un controllo dello stato calcolato.

- Implementa e gestisci i controlli sanitari per migliorare il rilevamento e ridurre le attività di manutenzione non necessarie.
  - Prima di associare un controllo sanitario a una protezione Shield Advanced, assicurati che sia in buono stato. L'associazione di un controllo dello stato che risulta non integro può alterare i meccanismi di rilevamento di Shield Advanced per le risorse protette.
  - Mantieni i tuoi controlli sanitari disponibili per l'uso da parte di Shield Advanced. Non eliminare un controllo dello stato di salute in Route 53 che stai utilizzando per una protezione Shield Advanced.
  - Usa gli ambienti di staging e test solo per testare i tuoi controlli sanitari. Mantieni le associazioni di controllo dello stato solo per ambienti che richiedono prestazioni e disponibilità a livello di produzione. Non mantenete l'associazione di controllo dello stato di salute in Shield Advanced per ambienti di staging e test.

Metriche comunemente utilizzate per i controlli sanitari

Questa sezione elenca le CloudWatch metriche di Amazon comunemente utilizzate nei controlli di integrità per misurare lo stato delle applicazioni durante gli eventi DDoS (Distributed Denial of Service). Per informazioni complete sui CloudWatch parametri per ogni tipo di risorsa, consulta l'elenco che segue la tabella.

Argomenti

- Metriche utilizzate per monitorare lo stato delle applicazioni

- CloudWatch Parametri Amazon per ogni tipo di risorsa

Metriche utilizzate per monitorare lo stato delle applicazioni

Risorsa	Parametro	Descrizione
Route 53	`HealthCheckStatus`	Lo stato dell'endpoint per il controllo dello stato di salute.
CloudFront	`5xxErrorRate`	La percentuale di tutte le richieste per le quali il codice di stato HTTP è 5xx. Ciò indica un attacco che ha un impatto sull'applicazione.
Application Load Balancer	`ActiveConnectionCount`	Il numero di connessioni TCP simultanee attive dai client al sistema di bilanciamento del carico e dal sistema di bilanciamento del carico agli obiettivi.
Application Load Balancer	`ConsumedLCUs`	Il numero di unità di capacità del sistema di bilanciamento del carico (LCU) utilizzate dal tuo sistema di bilanciamento del carico.

Application Load Balancer	`HTTPCode_ELB_4XX_Count`
	
	`HTTPCode_ELB_5XX_Count`
		Il numero di codici di errore del client HTTP 4xx o 5xx generati dal load balancer.

Application Load Balancer	`NewConnectionCount`	Il numero di nuove connessioni TCP stabilite dai client al sistema di bilanciamento del carico e dal sistema di

Risorsa	Parametro	Descrizione
		bilanciamento del carico alle destinazioni.
Application Load Balancer	`ProcessedBytes`	Il numero di byte elaborati dal sistema di bilanciamento del carico.
Application Load Balancer	`RejectedConnectionCount`	Il numero di connessioni che sono state rifiutate perché il sistema di bilanciamento del carico ha raggiunto il numero massimo di connessioni.
Application Load Balancer	`TargetConnectionErrorCount`	Il numero di connessioni che non sono state stabilite correttamente tra il sistema di bilanciamento del carico e la destinazione.
Application Load Balancer	`TargetResponseTime`	Il tempo trascorso, in secondi, dopo che la richiesta ha lasciato il sistema di bilanciamento del carico e quando riceve una risposta dalla destinazione.
Application Load Balancer	`UnHealthyHostCount`	Il numero di target considerati non integri.
Network Load Balancer	`ActiveFlowCount`	Il numero di connessioni TCP simultanee dai client alle destinazioni.

Risorsa	Parametro	Descrizione
Network Load Balancer	`ConsumedLCUs`	Il numero di unità di capacità del sistema di bilanciamento del carico (LCU) utilizzate dal tuo sistema di bilanciamento del carico.
Network Load Balancer	`NewFlowCount`	Il numero di nuove connessioni TCP stabilite dai client alle destinazioni.
Network Load Balancer	`PeakPacketsPerSecond`	Frequenza media di pacchetti più elevata (pacchetti elaborati al secondo), calcolata ogni 10 secondi durante la finestra di campionamento. Questo parametro include il traffico relativo ai controlli dell'integrità.
Network Load Balancer	`ProcessedBytes`	Il numero di byte elaborati dal sistema di bilanciamento del carico, incluse le intestazioni TCP/IP.
Global Accelerator	`NewFlowCount`	Il numero di nuove connessioni TCP stabilite dai client alle destinazioni.
Global Accelerator	`ProcessedBytesIn`	Il numero di byte in entrata elaborati dall'acceleratore, incluse le intestazioni TCP/IP.
Amazon EC2	`CPUUtilization`	La percentuale di unità di calcolo EC2 allocate attualmente in uso.

Risorsa	Parametro	Descrizione
Amazon EC2	`NetworkIn`	Il numero di byte ricevuti dall'istanza su tutte le interfacc e di rete.
Dimensionamento automatico Amazon EC2	`GroupMaxSize`	Dimensione massima del gruppo con scalabilità automatica.

CloudWatch Parametri Amazon per ogni tipo di risorsa

Per ulteriori informazioni sulle metriche disponibili per le risorse protette, consulta le seguenti sezioni nelle guide alle risorse:

- Amazon Route 53: monitoraggio delle risorse con i controlli di integrità di Amazon Route 53 e Amazon CloudWatch nella Amazon Route 53 Developer Guide.
- Amazon CloudFront — Monitoraggio CloudFront con Amazon CloudWatch nella Amazon CloudFront Developer Guide.
- Application Load Balancer: CloudWatch metriche per il tuo Application Load Balancer nella User Guide for Application Load Balancer.
- Network Load Balancer: CloudWatch metriche per il Network Load Balancer nella Guida per l'utente di Network Load Balancer.
- AWS Global Accelerator — Utilizzo di Amazon CloudWatch con AWS Global Accelerator la AWS Global Accelerator Developer Guide.
- Amazon Elastic Compute Cloud: elenca i CloudWatch parametri disponibili per le tue istanze in https://docs.aws.amazon.com/ 2/latest/ /. AWSEC UserGuide
- Amazon EC2 Auto Scaling: parametri di CloudWatch monitoraggio per i gruppi e le istanze di Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling.

Gestione delle associazioni di controllo sanitario

È possibile trarre il massimo vantaggio dall'utilizzo di un controllo dello stato di salute con Shield Advanced se il controllo dello stato segnala lo stato di salute solo quando l'applicazione è in esecuzione con parametri accettabili e segnala lo stato di salute solo quando non lo è. Utilizza le

indicazioni contenute in questa sezione per gestire le associazioni dei controlli sanitari in Shield Advanced.

> **Note**
>
> Shield Advanced non gestisce automaticamente i controlli sanitari.

Per utilizzare un controllo dello stato di salute con Shield Advanced è necessario quanto segue:

- Il controllo dello stato deve riportare lo stato di salute quando lo si associa alla protezione Shield Advanced.
- Il controllo sanitario deve essere pertinente allo stato di salute della risorsa protetta. L'utente è responsabile della definizione e del mantenimento dei controlli di integrità che riportino in modo accurato lo stato dell'applicazione, in base ai requisiti specifici dell'applicazione.
- Il controllo sanitario deve rimanere disponibile per l'uso da parte della protezione Shield Advanced. Non eliminare un controllo dello stato di salute in Route 53 che stai utilizzando per una protezione Shield Advanced.

Argomenti

Associare un controllo sanitario alla tua risorsa

La procedura seguente mostra come associare un controllo dello stato di Amazon Route 53 a una risorsa protetta.

> **Note**
>
> Prima di associare un controllo sanitario a una protezione Shield Advanced, assicurati che sia in buono stato. Per informazioni, consulta Monitoraggio dello stato dei controlli di integrità e ricezione delle notifiche nella Amazon Route 53 Developer Guide.

Per associare un controllo sanitario

1. Accedi AWS Management Console e apri la console AWS WAF & Shield all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel pannello AWS Shield di navigazione, scegli Risorse protette.
3. Nella scheda Protezioni, seleziona la risorsa che desideri associare a un controllo sanitario.
4. Scegli Configura protezioni.
5. Scegli Avanti fino ad arrivare alla pagina Configura il rilevamento DDoS basato sul controllo dello stato di salute (opzionale).
6. In Associated Health Check (Controllo stato associato), scegliere l'ID del controllo dello stato che si desidera associare alla protezione.

   > **Note**
   >
   > Se non vedi il controllo sanitario di cui hai bisogno, vai alla console Route 53 e verifica il controllo e il relativo ID. Per informazioni, consultare Creazione e aggiornamento di controlli dello stato.

7. Scorri il resto delle pagine fino a completare la configurazione. Nella pagina Protezioni, l'associazione di controllo sanitario aggiornata è elencata per la risorsa.
8. Nella pagina Protezioni, verifica che il nuovo controllo sanitario associato risulti integro.

   Non puoi iniziare a utilizzare correttamente un controllo dello stato di salute in Shield Advanced mentre il controllo dello stato segnala che non è integro. In questo modo Shield Advanced rileva falsi positivi a soglie molto basse e può anche influire negativamente sulla capacità dello Shield Response Team (SRT) di fornire un coinvolgimento proattivo per la risorsa.

   Se il nuovo controllo sanitario associato risulta non integro, procedi come segue:

   a. Dissocia il controllo dello stato dalla tua protezione in Shield Advanced.
   b. Rivedi le specifiche del controllo dello stato di salute in Amazon Route 53 e verifica le prestazioni e la disponibilità complessive dell'applicazione.
   c. Quando le prestazioni dell'applicazione rientrano nei parametri di buona salute e il controllo dello stato risulta corretto, riprova ad associare il controllo dello stato in Shield Advanced.

La procedura di associazione dei controlli sanitari è completa quando hai stabilito la tua nuova associazione per i controlli sanitari e risulta sana in Shield Advanced.

Dissociare un controllo sanitario dalla propria risorsa

La procedura seguente mostra come dissociare un controllo dello stato di Amazon Route 53 da una risorsa protetta.

Annullare l'associazione di un controllo sanitario

1. Accedi AWS Management Console e apri la console AWS WAF & Shield all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel pannello AWS Shield di navigazione, scegli Risorse protette.
3. Nella scheda Protezioni, seleziona la risorsa che desideri escludere da un controllo sanitario.
4. Scegli Configura protezioni.
5. Scegli Avanti fino ad arrivare alla pagina Configura il rilevamento DDoS basato sul controllo dello stato di salute (opzionale).
6. In Associated Health Check, scegli l'opzione vuota, elencata come -.
7. Scorri il resto delle pagine fino a completare la configurazione.

Nella pagina Protezioni, il campo relativo al controllo dello stato di salute della risorsa è impostato su -, a indicare che non vi è alcuna associazione tra i controlli sanitari.

Lo stato dell'associazione per il controllo dello stato di salute

Puoi vedere lo stato del controllo di integrità associato a una protezione nella pagina Risorse protette della console AWS WAF & Shield e nella pagina dei dettagli di ciascuna risorsa.

- Sano: il controllo sanitario è disponibile e riporta lo stato di salute.
- Non salutare: il controllo sanitario è disponibile e lo segnala come non salutare.
- Non disponibile: il controllo dello stato non è disponibile per l'uso da parte di Shield Advanced.

Per risolvere un controllo sanitario non disponibile

Crea e utilizza un nuovo controllo sanitario. Non provare ad associare nuovamente un controllo sanitario dopo che lo stato non è disponibile in Shield Advanced.

Per una guida dettagliata su come seguire questi passaggi, consulta gli argomenti precedenti.

1. In Shield Advanced, dissocia il controllo dello stato dalla risorsa.
2. In Route 53, crea un nuovo controllo dello stato della risorsa e annota il suo ID. Per informazioni, consulta Creating and Updating Health Checks nella Amazon Route 53 Developer Guide.
3. In Shield Advanced, associa il nuovo controllo dello stato alla risorsa.

Esempi di Health check

Questa sezione mostra esempi di controlli sanitari che è possibile utilizzare in un controllo sanitario calcolato. Un controllo sanitario calcolato utilizza una serie di controlli sanitari individuali per determinare uno stato combinato. Lo stato di ogni singolo controllo sanitario si basa sullo stato di un endpoint o sullo stato di una CloudWatch metrica Amazon. Combini i controlli sanitari in un controllo sanitario calcolato e quindi configuri il controllo sanitario calcolato per riportare lo stato di salute in base allo stato di salute combinato dei singoli controlli sanitari. Regola la sensibilità dei controlli sanitari calcolati in base ai requisiti di prestazioni e disponibilità delle applicazioni.

Per informazioni sui controlli sanitari calcolati, consulta Monitoraggio di altri controlli sanitari (controlli sanitari calcolati) nella Amazon Route 53 Developer Guide. Per ulteriori informazioni, consulta il post sul blog Route 53 Improvements — Calculated Health Checks and Latency Checks.

Argomenti

- CloudFront Distribuzioni Amazon
- Sistemi di load balancer
- Indirizzo IP elastico (EIP) di Amazon EC2

CloudFront Distribuzioni Amazon

Gli esempi seguenti descrivono i controlli sanitari che potrebbero essere combinati in un controllo sanitario calcolato per una CloudFront distribuzione:

- Monitora un endpoint specificando un nome di dominio in un percorso sulla distribuzione che fornisce contenuti dinamici. Una risposta valida includerebbe i codici di risposta HTTP 2xx e 3xx.
- Monitora lo stato di un CloudWatch allarme che misura lo stato dell' CloudFront origine. Ad esempio, puoi mantenere un CloudWatch allarme sulla metrica `TargetResponseTime` Application Load Balancer e creare un controllo dello stato che rifletta lo stato dell'allarme. Il controllo di integrità può non essere corretto quando il tempo di risposta, tra la richiesta che esce

dal sistema di bilanciamento del carico e il momento in cui il load balancer riceve una risposta dal bersaglio, supera la soglia configurata nell'allarme.

- Monitora lo stato di un CloudWatch allarme che misura la percentuale di richieste per cui il codice di stato HTTP della risposta è 5xx. Se il tasso di errore 5xx della CloudFront distribuzione è superiore alla soglia definita nell' CloudWatch allarme, lo stato di questo controllo sanitario diventerà non integro.

Sistemi di load balancer

Gli esempi seguenti descrivono i controlli di integrità che potrebbero essere utilizzati nei controlli di integrità calcolati per un acceleratore standard Application Load Balancer, Network Load Balancer o Global Accelerator.

- Monitora lo stato di un CloudWatch allarme che misura il numero di nuove connessioni stabilite dai client al sistema di bilanciamento del carico. È possibile impostare la soglia di allarme per il numero medio di nuove connessioni in una certa misura superiore alla media giornaliera. Le metriche per ogni tipo di risorsa sono le seguenti:
  - Application Load Balancer: `NewConnectionCount`
  - Network Load Balancer: `ActiveFlowCount`
  - Acceleratore globale: `NewFlowCount`
- Per Application Load Balancer e Network Load Balancer, monitora lo stato di CloudWatch un allarme che misura il numero di sistemi di bilanciamento del carico considerati integri. È possibile impostare la soglia di allarme sulla zona di disponibilità o sul numero minimo di host integri richiesto dal sistema di bilanciamento del carico. Le metriche disponibili per le risorse del load balancer sono le seguenti:
  - Application Load Balancer: `HealthyHostCount`
  - Network Load Balancer: `HealthyHostCount`
- Per Application Load Balancer, monitora lo stato di un CloudWatch allarme che misura il numero di codici di risposta HTTP 5xx generati dagli obiettivi del load balancer. Per un Application Load Balancer, puoi utilizzare la metrica `HTTPCode_Target_5XX_Count` e basare la soglia di allarme sulla somma di tutti gli errori 5xx per il load balancer.

Indirizzo IP elastico (EIP) di Amazon EC2

I seguenti esempi di controlli dello stato possono essere combinati in un controllo dello stato calcolato per un indirizzo IP elastico Amazon EC2:

- Monitora un endpoint specificando un indirizzo IP sull'indirizzo IP elastico. Il controllo dello stato rimarrà valido finché sarà possibile stabilire una connessione TCP con la risorsa associata all'indirizzo IP.
- Monitora lo stato di un CloudWatch allarme che misura la percentuale di unità di calcolo Amazon EC2 allocate attualmente in uso sull'istanza. Puoi utilizzare il parametro Amazon EC2 `CPUUtilization` e basare la soglia di allarme su quello che consideri un elevato tasso di utilizzo della CPU per la tua applicazione, ad esempio il 90%.

Gestione della protezione delle risorse in AWS Shield Advanced

Utilizza le indicazioni in questa sezione per gestire le protezioni Shield Advanced per le tue risorse.

> **Note**
>
> Shield Advanced protegge solo le risorse specificate in Shield Advanced o tramite una politica AWS Firewall Manager Shield Advanced. Non protegge automaticamente le risorse.

Se utilizzi una policy AWS Firewall Manager Shield Advanced, non è necessario gestire le protezioni per le risorse che rientrano nell'ambito della policy. Firewall Manager gestisce automaticamente le protezioni per gli account e le risorse che rientrano nell'ambito di una policy, in base alla configurazione della policy. Per ulteriori informazioni, consulta AWS Shield Advanced politiche.

Argomenti

- Aggiungere AWS Shield Advanced protezione alle risorse AWS
- Configurazione delle protezioni AWS Shield Advanced
- Rimuovere AWS Shield Advanced la protezione da una AWS risorsa

Aggiungere AWS Shield Advanced protezione alle risorse AWS

Segui le indicazioni in questa sezione per aggiungere la protezione Shield Advanced a una o più risorse.

Per aggiungere protezione a una AWS risorsa

1. Accedi AWS Management Console e apri la console AWS WAF & Shield all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel pannello di navigazione, sotto AWS Shield scegli Risorse protette.
3. Scegli Aggiungi risorse da proteggere.
4. Nella pagina Scegli le risorse da proteggere con Shield Advanced, in Specificare la regione e i tipi di risorse, fornisci le specifiche della regione e del tipo di risorsa per le risorse che desideri proteggere. È possibile proteggere le risorse in più regioni selezionando Tutte le regioni e restringere la selezione alle risorse globali selezionando Globale. È possibile deselezionare tutti i tipi di risorse che non si desidera proteggere. Per informazioni sulle protezioni per i tipi di risorse, consulta. AWS Shield Advanced protezioni per tipo di risorsa
5. Scegli Carica risorse. Shield Advanced compila la sezione Seleziona risorse con le AWS risorse che corrispondono ai tuoi criteri.
6. Nella sezione Seleziona risorse, puoi filtrare l'elenco delle risorse inserendo una stringa da cercare negli elenchi delle risorse.

   Seleziona le risorse che desideri proteggere.
7. Nella sezione Tag, se desideri aggiungere tag alle protezioni Shield Advanced che stai creando, specificali. Per informazioni sull'etichettatura AWS delle risorse, consulta Lavorare con Tag Editor.
8. Scegli Proteggi con Shield Advanced. Ciò aggiunge le protezioni Shield Advanced alle risorse.

Configurazione delle protezioni AWS Shield Advanced

Puoi modificare le impostazioni delle tue AWS Shield Advanced protezioni in qualsiasi momento. Per fare ciò, consulta le opzioni per le protezioni selezionate e modifica le impostazioni che devi modificare.

Per gestire le risorse protette

1. Accedi AWS Management Console e apri la console AWS WAF & Shield all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel pannello AWS Shield di navigazione, scegli Risorse protette.
3. Nella scheda Protezioni, seleziona le risorse che desideri proteggere.
4. Scegli Configura le protezioni e l'opzione di specifica delle risorse che desideri.

5. Esamina ciascuna delle opzioni di protezione delle risorse, apportando le modifiche necessarie.

Configura le protezioni DDoS a livello di applicazione

Per proteggerti dagli attacchi alle risorse Amazon CloudFront e Application Load Balancer, puoi aggiungere ACL AWS WAF Web e aggiungere regole basate sulla frequenza. Per informazioni a riguardo, consulta. ACL AWS WAF Web Shield Advanced a livello applicativo e regole basate sulla velocità

Puoi anche abilitare la mitigazione automatica degli attacchi DDoS a livello di applicazione Shield Advanced. Per informazioni su come AWS WAF funziona, consulta. AWS WAF Per informazioni sulla funzionalità di mitigazione automatica, vedereMitigazione DDoS automatica a livello di applicazione Shield Advanced.

> **Important**
>
> Se gestisci le tue protezioni Shield Advanced AWS Firewall Manager utilizzando una policy Shield Advanced, non puoi gestire le protezioni a livello di applicazione qui. Per tutte le altre risorse, consigliamo di allegare almeno un ACL Web a ciascuna risorsa, anche se l'ACL Web non contiene alcuna regola.

> **Note**
>
> Quando abiliti la mitigazione automatica degli attacchi DDoS a livello di applicazione per una risorsa, se necessario, l'operazione aggiunge automaticamente un ruolo collegato al servizio all'account per fornire a Shield Advanced le autorizzazioni necessarie per gestire le protezioni ACL Web. Per informazioni, consulta Utilizzo di ruoli collegati ai servizi per Shield Advanced.

Per configurare le protezioni DDoS a livello di applicazione

1. Nella pagina Configura le protezioni DDoS di livello 7, se la risorsa non è già associata a un ACL Web, puoi scegliere un ACL Web esistente o crearne uno personalizzato.

   Per creare un'ACL Web, seguire queste fasi:

   a. Scegliere Create web ACL (Crea ACL Web).

b. Inserire un nome. Non è possibile modificare il nome dopo aver creato l'ACL Web.

c. Scegli Crea.

> **Note**
>
> Se una risorsa è già associata a un'ACL Web, non è possibile modificarla in un'ACL Web differente. Se si desidera modificare l'ACL Web, in primo luogo è necessario rimuovere le ACL Web associate dalla risorsa. Per ulteriori informazioni, consulta Associazione o dissociazione di un ACL Web con una risorsa AWS.

2. Se l'ACL web non ha una regola basata sulla tariffa definita, puoi aggiungerne una scegliendo Aggiungi regola limite di velocità e quindi eseguendo i seguenti passaggi:

   a. Inserire un nome.

   b. Inserire un limite di frequenza Questo è il numero massimo di richieste consentite in un periodo di cinque minuti da un singolo indirizzo IP prima che l'azione della regola basata sulla frequenza venga applicata all'indirizzo IP. Quando le richieste provenienti dall'indirizzo IP scendono al di sotto del limite, l'azione viene interrotta.

   c. Imposta l'azione della regola per contare o bloccare le richieste provenienti dagli indirizzi IP quando il numero delle richieste supera il limite. L'applicazione e la rimozione dell'azione della regola potrebbero avere effetto uno o due minuti dopo la modifica della frequenza di richiesta dell'indirizzo IP.

   d. Scegli Aggiungi regola.

3. Per la mitigazione automatica degli attacchi DDoS a livello di applicazione, scegli se vuoi che Shield Advanced mitighi automaticamente gli attacchi DDoS per tuo conto, come segue:

   - Per abilitare la mitigazione automatica, scegli Abilita, quindi seleziona l'azione della AWS WAF regola che desideri che Shield Advanced utilizzi nelle sue regole personalizzate. Le tue scelte sono Count e. Block Per informazioni su queste azioni delle AWS WAF regole, vedereOperazione delle regole. Per informazioni su come Shield Advanced gestisce questa impostazione di azione, vedereIn che modo Shield Advanced gestisce l'impostazione delle azioni delle regole.
   - Per disabilitare la mitigazione automatica, scegli Disabilita.
   - Per lasciare invariate le impostazioni di mitigazione automatica per le risorse che gestisci, lascia la scelta predefinita Mantieni le impostazioni correnti.

Per informazioni sulla mitigazione automatica degli attacchi DDoS a livello di applicazione Shield Advanced, vedere. Mitigazione DDoS automatica a livello di applicazione Shield Advanced

4. Seleziona Successivo.

Crea allarmi e notifiche

La procedura seguente mostra come gestire gli CloudWatch allarmi per le risorse protette.

> **Note**
>
> CloudWatch comporta costi aggiuntivi. Per CloudWatch i prezzi, consulta la pagina CloudWatch dei prezzi di Amazon.

Per creare allarmi e notifiche

1. Nella pagina delle protezioni Crea allarmi e notifiche: facoltativo, configura gli argomenti SNS per gli allarmi e le notifiche che desideri ricevere. Per le risorse per le quali non si desidera ricevere notifiche, scegliere No topic (Nessun argomento). Puoi aggiungere un argomento Amazon SNS o crearne uno nuovo.
2. Per creare un argomento su Amazon SNS, segui questi passaggi:
   a. Nell'elenco a discesa, scegli Crea un argomento SNS.
   b. Inserisci un nome dell'argomento.
   c. Facoltativamente, inserisci un indirizzo e-mail a cui verranno inviati i messaggi Amazon SNS, quindi scegli Aggiungi e-mail. Puoi inserirne più di uno.
   d. Scegli Crea.
3. Seleziona Successivo.

Rimuovere AWS Shield Advanced la protezione da una AWS risorsa

Puoi rimuovere AWS Shield Advanced la protezione da qualsiasi AWS risorsa in qualsiasi momento.

> **Important**
>
> L'eliminazione di una AWS risorsa non rimuove la risorsa da AWS Shield Advanced. È inoltre necessario rimuovere la protezione sulla risorsa da AWS Shield Advanced, come descritto in questa procedura.

Rimuovere AWS Shield Advanced la protezione da una AWS risorsa

1. Accedi AWS Management Console e apri la console AWS WAF & Shield all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel pannello AWS Shield di navigazione, scegli Risorse protette.
3. Nella scheda Protezioni, seleziona le risorse di cui desideri rimuovere le protezioni.
4. Scegli Elimina protezioni.
   - Se hai un CloudWatch allarme Amazon configurato per una protezione, hai la possibilità di eliminare l'allarme insieme alla protezione. Se scegli di non eliminare l'allarme a questo punto, puoi invece eliminarlo in un secondo momento utilizzando la CloudWatch console.

> **Note**
>
> Per le protezioni per cui è configurato un controllo dello stato di Amazon Route 53, se aggiungi nuovamente la protezione in un secondo momento, la protezione include comunque il controllo dello stato.

I passaggi precedenti rimuovono la AWS Shield Advanced protezione da risorse specifiche AWS . Non annullano il tuo AWS Shield Advanced abbonamento. Continueranno a essere addebitati costi per il servizio. Per informazioni sull' AWS Shield Advanced abbonamento, contatta il AWS Support Centro.

Rimuovere un CloudWatch allarme dalle protezioni Shield Advanced

Per rimuovere un CloudWatch allarme dalle protezioni Shield Advanced, esegui una delle seguenti operazioni:

- Eliminare la protezione come descritto su Rimuovere AWS Shield Advanced la protezione da una AWS risorsa. Assicurarsi di aver selezionato la casella di controllo accanto alla voce Also delete related DDoSDetection alarm (Elimina anche i relativi allarmi DDoSDetection).
- Elimina l'allarme utilizzando la CloudWatch console. Il nome dell'allarme da eliminare inizia con DDoS DetectedAlarmForProtection.

AWS Shield Advanced gruppi di protezione

Utilizza i gruppi di protezione per creare raccolte logiche delle risorse protette e gestirne le protezioni come gruppo. Per informazioni sulla gestione della protezione delle risorse, vedere. Configurazione delle protezioni AWS Shield Advanced

> **Note**
>
> La mitigazione automatica degli attacchi DDoS a livello di applicazione non interagisce con i gruppi di protezione. È possibile abilitare la mitigazione automatica per le risorse che si trovano nei gruppi di protezione, ma Shield Advanced non applica automaticamente le mitigazioni degli attacchi in base ai risultati dei gruppi di protezione. Shield Advanced applica mitigazioni automatiche degli attacchi per le singole risorse.

AWS Shield Advanced i gruppi di protezione offrono una soluzione self-service per personalizzare l'ambito di rilevamento e mitigazione trattando più risorse protette come un'unica unità. Il raggruppamento delle risorse può offrire una serie di vantaggi.

- Migliora la precisione del rilevamento.
- Riduci le notifiche di eventi irrealizzabili.
- Aumenta la copertura delle azioni di mitigazione per includere risorse protette che potrebbero essere colpite anche durante un evento.
- Accelera i tempi di mitigazione degli attacchi con più obiettivi simili.
- Facilita la protezione automatica delle risorse protette appena create.

I gruppi di protezione possono contribuire a ridurre i falsi positivi in situazioni come lo scambio tra blu e verde, in cui le risorse alternano un carico vicino allo zero e uno a pieno carico. Un altro esempio è quando si creano ed eliminano risorse frequentemente mantenendo un livello di carico condiviso tra i

membri del gruppo. In situazioni come queste, il monitoraggio delle singole risorse può portare a falsi positivi, mentre il monitoraggio dello stato del gruppo di risorse no.

È possibile configurare i gruppi di protezione in modo da includere tutte le risorse protette, tutte le risorse di tipi di risorse specifici o risorse specificate individualmente. Le nuove risorse protette che soddisfano i criteri del gruppo di protezione vengono automaticamente incluse nel gruppo di protezione. Una risorsa protetta può appartenere a più gruppi di protezione.

Gestione dei gruppi di AWS Shield Advanced protezione

Utilizza le indicazioni contenute in questa sezione per gestire le configurazioni dei gruppi di protezione.

Creazione di un gruppo di protezione Shield Advanced

Per creare un gruppo di protezione

1. Accedi AWS Management Console e apri la console AWS WAF & Shield all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel pannello AWS Shield di navigazione, scegli Risorse protette.
3. Scegli la scheda Gruppi di protezione, quindi scegli Crea gruppo di protezione.
4. Nella pagina Crea gruppo di protezione, fornisci un nome per il tuo gruppo. Utilizzerai questo nome per identificare il gruppo nell'elenco delle risorse protette. Non è possibile modificare il nome di un gruppo di protezione dopo averlo creato.
5. Per i criteri di raggruppamento della protezione, selezionare i criteri che Shield Advanced deve utilizzare per identificare le risorse protette da includere nel gruppo. Effettua le tue selezioni aggiuntive in base ai criteri che hai scelto.
6. Per Aggregazione, seleziona il modo in cui desideri che Shield Advanced combini i dati delle risorse per il gruppo al fine di rilevare, mitigare e segnalare gli eventi.

   - Somma: utilizza il traffico totale all'interno del gruppo. Questa è una buona scelta per la maggior parte dei casi. Gli esempi includono indirizzi IP elastici per istanze Amazon EC2 con scalabilità manuale o automatica.
   - Media: utilizza la media del traffico all'interno del gruppo. Questa è una buona scelta per le risorse che condividono il traffico in modo uniforme. Gli esempi includono acceleratori e sistemi di bilanciamento del carico.
   - Max: utilizza il traffico più elevato proveniente da ciascuna risorsa. Ciò è utile per le risorse che non condividono il traffico e per le risorse che condividono il traffico in modo non uniforme. Gli

esempi includono CloudFront le distribuzioni Amazon e le risorse di origine per le CloudFront distribuzioni.

7. Scegli Salva per salvare il tuo gruppo di protezione e tornare alla pagina Risorse protette.

Nella pagina Shield Events, puoi visualizzare gli eventi per il tuo gruppo di protezione ed espandere la visualizzazione di informazioni aggiuntive sulle risorse protette che fanno parte del gruppo.

Aggiornamento di un gruppo di protezione Shield Advanced

Per aggiornare un gruppo di protezione

1. Accedi AWS Management Console e apri la console AWS WAF & Shield all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel pannello AWS Shield di navigazione, scegli Risorse protette.
3. Nella scheda Gruppi di protezione, seleziona la casella di controllo accanto al gruppo di protezione che desideri modificare.
4. Nella pagina del gruppo di protezione, scegli Modifica. Apporta le modifiche alle impostazioni del gruppo di protezione.
5. Scegliere Salva per salvare le modifiche.

Eliminazione di un gruppo di protezione Shield Advanced

Per eliminare un gruppo di protezione

1. Accedi AWS Management Console e apri la console AWS WAF & Shield all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel pannello AWS Shield di navigazione, scegli Risorse protette.
3. Nella scheda Gruppi di protezione, seleziona la casella di controllo accanto al gruppo di protezione che desideri rimuovere.
4. Nella pagina del gruppo di protezione, scegli Elimina e conferma l'azione.

Monitoraggio delle modifiche alla protezione delle risorse in AWS Config

È possibile registrare le modifiche alla AWS Shield Advanced protezione delle risorse utilizzando AWS Config. Puoi utilizzare queste informazioni per conservare una cronologia delle modifiche di configurazione per eventuali audit e per la risoluzione dei problemi.

Per registrare le modifiche alla protezione, abilitalo AWS Config per ogni risorsa che desideri monitorare. Per ulteriori informazioni, consulta Nozioni di base su AWS Config nella AWS Config Guida per gli sviluppatori.

È necessario AWS Config abilitarlo per ogni risorsa Regione AWS che contiene le risorse tracciate. È possibile abilitare AWS Config manualmente oppure utilizzare il AWS CloudFormation modello «Enable AWS Config» in AWS CloudFormation StackSets Sample Templates nella Guida per l'AWS CloudFormation utente.

Se abiliti AWS Config, ti verranno addebitati i costi come indicato nella pagina AWS Config Prezzi.

> **Note**
>
> Se hai già AWS Config abilitato le regioni e le risorse necessarie, non devi fare nulla. AWS Config i registri relativi alle modifiche alla protezione delle risorse iniziano a essere compilati automaticamente.

Dopo l'attivazione AWS Config, utilizza la regione Stati Uniti orientali (Virginia settentrionale) nella AWS Config console per visualizzare la cronologia delle modifiche alla configurazione per AWS Shield Advanced le risorse globali.

Visualizza la cronologia delle modifiche per le risorse AWS Shield Advanced regionali tramite la AWS Config console nelle regioni Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), Europa (Irlanda), Europa (Francoforte), Asia Pacifico (Tokyo) e Asia Pacifico (Sydney).

Visibilità sugli eventi DDoS

AWS Shield offre visibilità nelle seguenti categorie di eventi e attività legate agli eventi:

- Globale: tutti i clienti possono accedere a una visione aggregata dell'attività globale delle minacce nelle ultime due settimane. Puoi visualizzare queste informazioni nelle pagine Getting Started e Global Threat dashboard della AWS Shield console. Per ulteriori informazioni, consulta AWS Shield attività globale e dell'account.
- Account: tutti i clienti possono accedere a un riepilogo degli eventi relativi al proprio account nell'anno precedente. Puoi visualizzare queste informazioni nella pagina Guida introduttiva della AWS Shield console. Per ulteriori informazioni, consulta AWS Shield attività globale e dell'account.

Quando ti abboni a Shield Advanced e aggiungi protezioni alle tue risorse, accedi a informazioni aggiuntive sugli eventi e gli attacchi DDoS alle risorse protette:

- Eventi su risorse protette: Shield Advanced fornisce informazioni dettagliate per ogni evento tramite la pagina Eventi della AWS Shield console. Per ulteriori informazioni, consulta AWS Shield Advanced eventi.
- Metriche degli eventi per risorse protette: Shield Advanced pubblica i CloudWatch parametri di rilevamento, mitigazione e i principali contributori di Amazon per tutte le risorse che protegge. Puoi utilizzare queste metriche per configurare dashboard e allarmi. CloudWatch Per ulteriori informazioni, consulta AWS Shield Advanced metriche.
- Visibilità degli eventi su più account per le risorse protette: se utilizzi AWS Firewall Manager per gestire le protezioni Shield Advanced, puoi abilitare la visibilità delle protezioni su più account utilizzando Firewall Manager in combinazione con. AWS Security Hub Per ulteriori informazioni, consulta Visibilità degli eventi su tutti gli account.

Se abiliti la mitigazione automatica degli attacchi DDoS a livello di applicazione per una protezione a livello di applicazione,

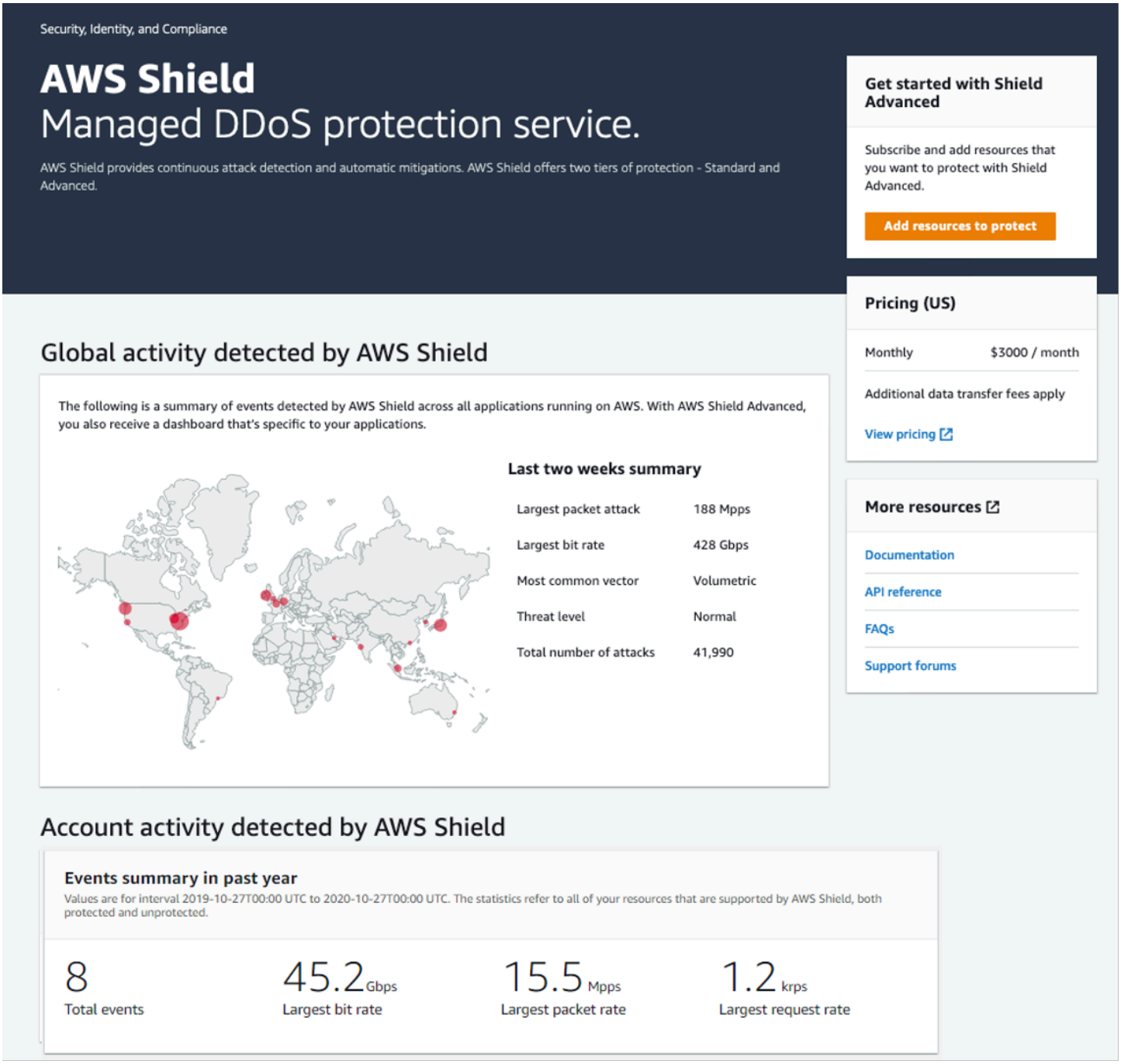
Argomenti

- AWS Shield attività globale e dell'account
- AWS Shield Advanced eventi
- Visibilità degli eventi su tutti gli account

AWS Shield attività globale e dell'account

Puoi accedere a una visualizzazione aggregata dell'attività globale delle minacce e a un riepilogo degli eventi per account nelle pagine Getting Started della AWS Shield console e Global threat dashboard.

La schermata seguente mostra un esempio di pagina Getting Started.



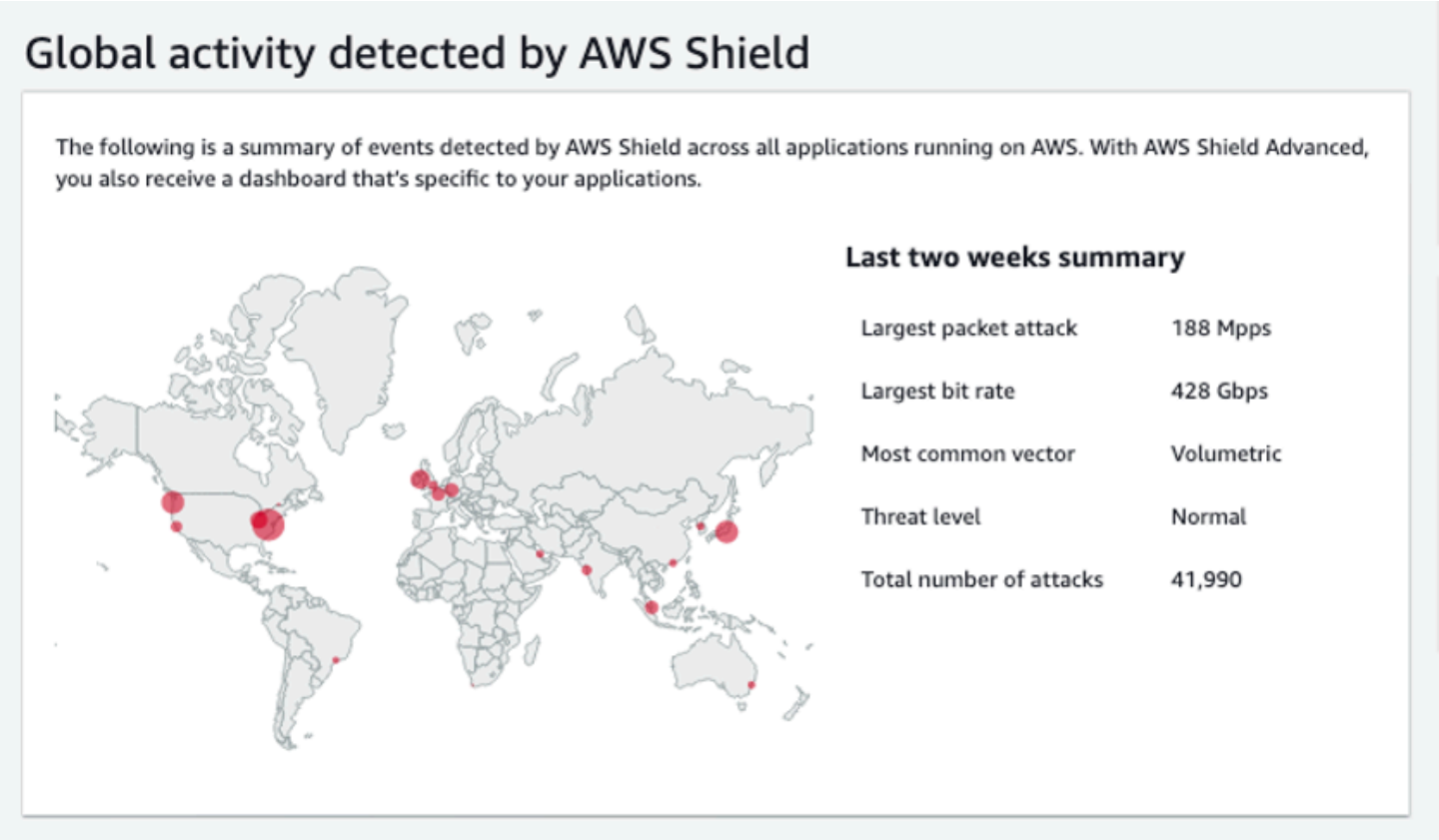
Per accedere alla console AWS Shield

- Accedi AWS Management Console e apri la console AWS WAF & Shield all'[indirizzo https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/).

Non è necessario un abbonamento a Shield Advanced per accedere alle informazioni di riepilogo delle attività globali e degli eventi dell'account.

Attività globale

Queste informazioni sono disponibili tramite la AWS Shield console Global Threat dashboard e le pagine Getting Started. La schermata seguente mostra un esempio del riquadro delle attività globali.



L'attività globale descrive gli eventi DDoS osservati in tutti i clienti. AWS Una volta all'ora, AWS aggiorna le informazioni per le due settimane precedenti. Nel riquadro della console, puoi vedere i risultati, suddivisi per AWS regione e visualizzati su una mappa termica mondiale. Accanto alla mappa, Shield visualizza informazioni di riepilogo come l'attacco a pacchetto più grande, il bit rate più elevato, il vettore più comune, il numero totale di attacchi e il livello di minaccia. Il livello di minaccia è una valutazione dell'attuale attività globale rispetto a quella AWS normalmente osservata. Il valore predefinito del livello di minaccia è Normale. AWS aggiorna automaticamente il valore su Alto per attività DDoS elevate.

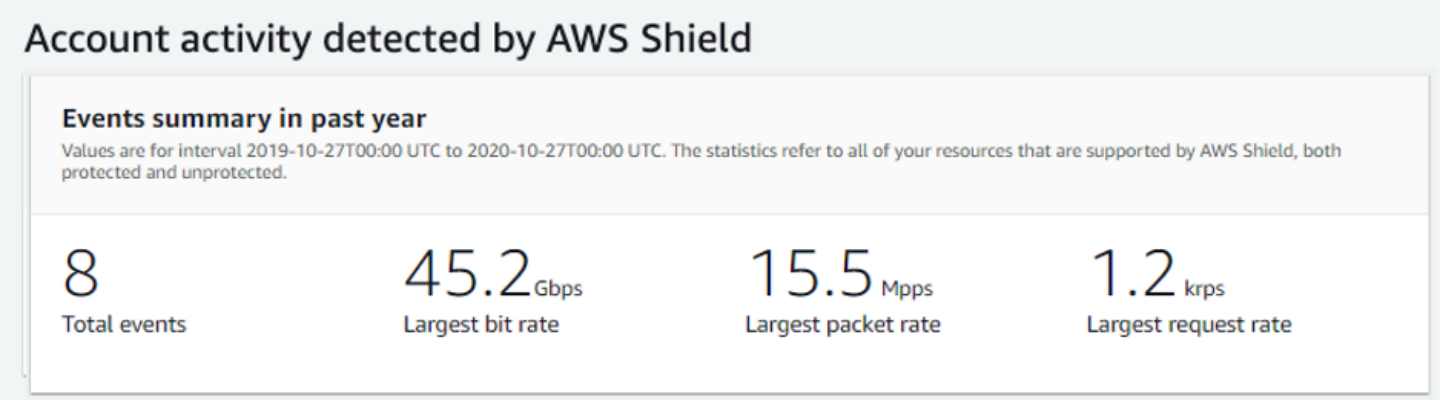
Il pannello di controllo delle minacce globali fornisce anche metriche relative alle serie temporali e offre la possibilità di passare da una durata all'altra. Per visualizzare la cronologia degli attacchi DDoS significativi, puoi personalizzare la dashboard per visualizzare le visualizzazioni dall'ultimo giorno alle ultime due settimane. Le metriche relative alle serie temporali forniscono una visualizzazione del bit rate, della frequenza dei pacchetti o della frequenza di richiesta massimi

per tutti gli eventi rilevati da AWS Shield per le applicazioni in esecuzione AWS durante la finestra temporale selezionata.

Attività dell'account

Queste informazioni sono disponibili nella pagina Getting AWS Shield Started della console.

La schermata seguente mostra un esempio di riquadro delle attività dell'account.



L'attività dell'account descrive gli eventi DDoS rilevati da Shield per le risorse idonee alla protezione da parte di Shield Advanced. Ogni giorno, Shield crea metriche di riepilogo per l'anno che termina alle 00:00 UTC del giorno precedente, quindi visualizza gli eventi totali, la velocità di trasmissione massima, la frequenza di pacchetti massima e la frequenza di richiesta massima.

- La metrica degli eventi totali riflette ogni volta che Shield ha rilevato attributi sospetti nel traffico destinato alla tua applicazione. Gli attributi sospetti possono includere traffico con un volume superiore al normale, traffico che non corrisponde al profilo storico dell'applicazione o traffico che non corrisponde alle euristiche definite da Shield per il traffico applicativo valido.
- Per ogni risorsa sono disponibili le statistiche relative alla velocità in bit e alla velocità di pacchetto più elevata.
- La statistica sulla frequenza di richiesta massima è disponibile solo per CloudFront le distribuzioni Amazon e gli Application Load Balancer a cui è associato un ACL Web. AWS WAF

> **Note**
>
> Puoi anche accedere al riepilogo degli eventi a livello di account tramite l'operazione API. AWS Shield DescribeAttackStatistics

AWS Shield Advanced eventi

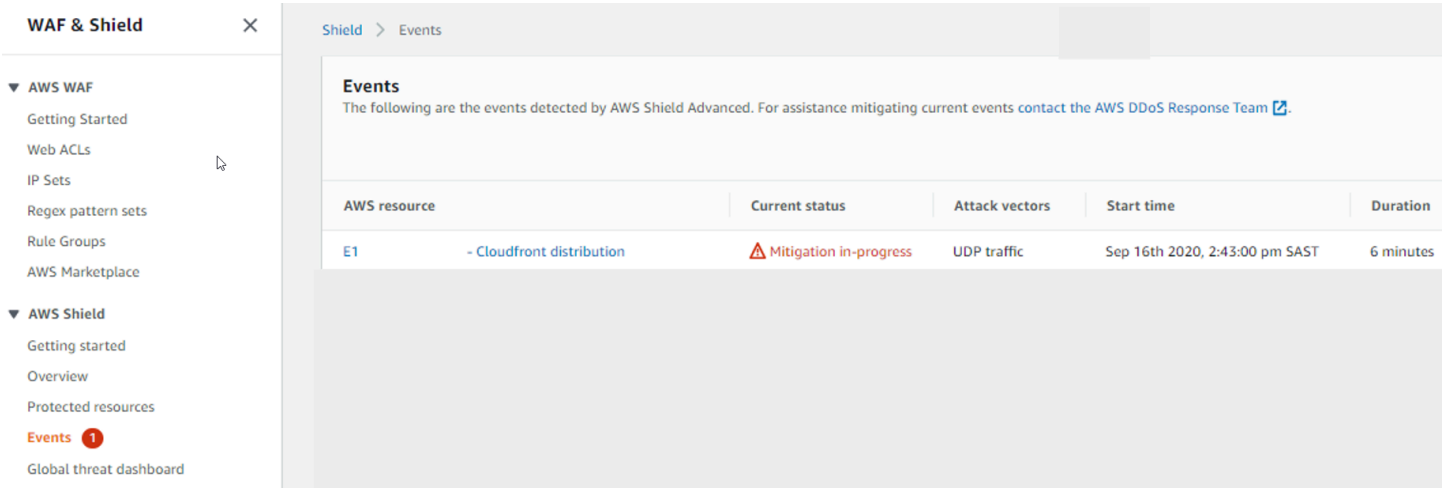
Quando ti abboni a Shield Advanced e proteggi le tue risorse, accedi a funzionalità di visibilità aggiuntive per le risorse. Questi includono la notifica quasi in tempo reale degli eventi rilevati da Shield Advanced e informazioni aggiuntive sugli eventi rilevati e sulle mitigazioni.

> **Note**
>
> Le informazioni sugli eventi nella console Shield Advanced si basano sulle metriche di Shield Advanced. Per informazioni sulle metriche Shield Advanced, consulta AWS Shield Advanced metriche

AWS Shield valuta il traffico verso la risorsa protetta secondo più dimensioni. Quando viene rilevata un'anomalia, Shield Advanced crea un evento separato per ogni risorsa interessata.

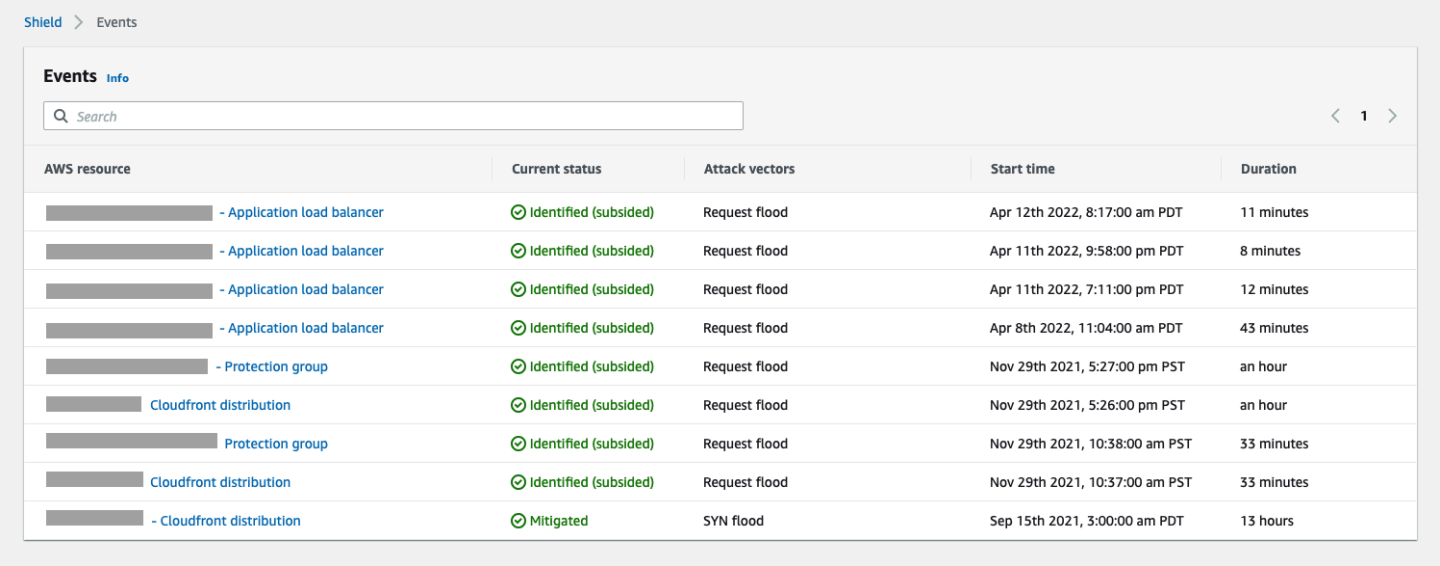
Puoi accedere ai riepiloghi e ai dettagli degli eventi tramite la pagina Eventi della console Shield. La pagina Eventi di primo livello fornisce una panoramica degli eventi attuali e passati.

La schermata seguente mostra un esempio di pagina Eventi con un singolo evento in corso. Questo evento attivo è contrassegnato anche nel riquadro di navigazione a sinistra.



Shield Advanced potrebbe anche adottare automaticamente misure di mitigazione contro gli attacchi, a seconda del tipo di traffico e delle protezioni configurate. Queste mitigazioni possono proteggere la tua risorsa dalla ricezione di traffico in eccesso o dal traffico che corrisponde a una firma nota di attacco DDoS.

La schermata seguente mostra un esempio di elenco degli eventi in cui tutti gli eventi sono stati mitigati da Shield Advanced o si sono attenuati da soli.



Proteggi le tue risorse prima di un evento

Migliora la precisione del rilevamento degli eventi proteggendo le risorse con Shield Advanced mentre ricevono il normale traffico previsto, prima che siano soggette a un attacco DDoS.

Per segnalare con precisione gli eventi relativi a una risorsa protetta, Shield Advanced deve innanzitutto stabilire una linea di base dei modelli di traffico previsti per tale risorsa.

- Shield Advanced segnala gli eventi a livello di infrastruttura per le risorse dopo che sono state protette per almeno 15 minuti.
- Shield Advanced segnala gli eventi a livello di applicazione Web per le risorse dopo che sono state protette per almeno 24 ore. La precisione del rilevamento degli eventi a livello di applicazione è ottimale dopo che Shield Advanced ha osservato il traffico previsto per 30 giorni.

Per accedere alle informazioni sugli eventi nella AWS Shield console

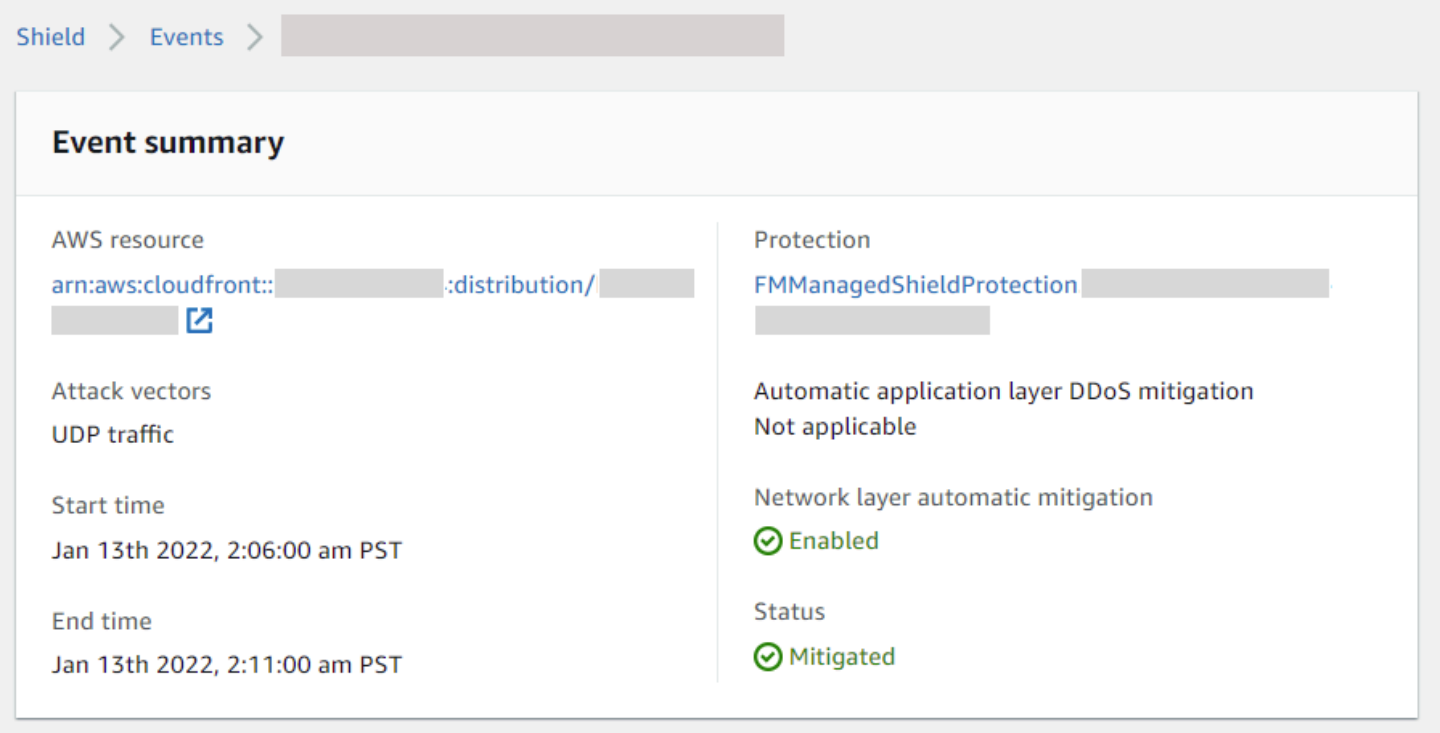
1. Accedi AWS Management Console e apri la console AWS WAF & Shield all'indirizzo https://console.aws.amazon.com/wafv2/.
2. Nel pannello AWS Shield di navigazione, scegli Eventi. La console mostra la pagina Eventi.
3. Dalla pagina Eventi, puoi selezionare qualsiasi evento nell'elenco per visualizzare ulteriori informazioni di riepilogo e dettagli sull'evento.

Argomenti

AWS Shield Advanced riassunti degli eventi

Puoi visualizzare informazioni di riepilogo e dettagli su un evento nella pagina della console dell'evento. Per aprire la pagina di un evento, selezionate il nome della AWS risorsa dall'elenco delle pagine Eventi.

La schermata seguente mostra un esempio di riepilogo di un evento a livello di rete.



Le informazioni di riepilogo della pagina dell'evento includono quanto segue.

- Stato attuale: valori che indicano lo stato dell'evento e le azioni intraprese da Shield Advanced sull'evento. I valori di stato si applicano agli eventi a livello di infrastruttura (livello 3 o 4) e a livello di applicazione (livello 7).
  - Identificato (in corso) e Identificato (attenuato): indicano che Shield Advanced ha rilevato un evento, ma finora non ha intrapreso alcuna azione al riguardo. Identificato (attenuato) indica che il traffico sospetto rilevato da Shield si è interrotto senza intervento.

  - Attenuazione in corso e mitigata: indicano che Shield Advanced ha rilevato un evento e ha preso provvedimenti in merito. Mitigated viene utilizzato anche quando la risorsa di destinazione è una CloudFront distribuzione Amazon o una zona ospitata di Amazon Route 53, che dispongono di mitigazioni automatiche in linea.
- Vettori di attacco: vettori di attacco DDoS come TCP SYN flood ed euristiche di rilevamento Shield Advanced come request flood. Questi possono essere indicatori di un attacco DDoS.
- Ora di inizio: la data e l'ora in cui è stato rilevato il primo punto dati anomalo sul traffico.
- Durata o ora di fine: indica il tempo trascorso tra l'ora di inizio dell'evento e l'ultimo punto dati anomalo osservato da Shield Advanced. Mentre un evento è in corso, questi valori continueranno ad aumentare.
- Protezione: assegna un nome alla protezione Shield Advanced associata alla risorsa e fornisce un collegamento alla relativa pagina di protezione. È disponibile nella pagina del singolo evento.
- Mitigazione DDoS automatica a livello di applicazione: utilizzata per la protezione a livello di applicazione, per indicare se la mitigazione DDoS a livello di applicazione automatica Shield Advanced è abilitata per la risorsa. Se è abilitata, fornisce un collegamento per accedere e gestire la configurazione. È disponibile nella pagina del singolo evento.
- Attenuazione automatica a livello di rete: indica se la risorsa dispone di una mitigazione automatica a livello di rete. Se una risorsa ha un componente a livello di rete, lo avrà abilitato. Queste informazioni sono disponibili nella pagina del singolo evento.

Per le risorse che vengono spesso prese di mira, Shield può lasciare in atto delle mitigazioni dopo che il traffico in eccesso si è attenuato, per prevenire ulteriori eventi ricorrenti.

> **Note**
>
> Puoi anche accedere ai riepiloghi degli eventi per le risorse protette tramite l'operazione API. AWS Shield ListAttacks

AWS Shield Advanced dettagli dell'evento

Puoi visualizzare i dettagli sul rilevamento e la mitigazione di un evento e sui principali contributori nella sezione inferiore della pagina della console relativa all'evento. Questa sezione può includere una combinazione di traffico legittimo e potenzialmente indesiderato e può rappresentare sia il traffico passato alla risorsa protetta sia il traffico bloccato dalle mitigazioni Shield.

- Rilevamento e mitigazione: fornisce informazioni sull'evento osservato e sulle eventuali misure di mitigazione applicate a tale evento. Per informazioni sulla mitigazione degli eventi, vedere. Risposta agli eventi DDoS
- Collaboratori principali: classifica il traffico coinvolto nell'evento ed elenca le fonti di traffico principali che Shield ha identificato per ciascuna categoria. Per gli eventi a livello di applicazione, utilizza le informazioni dei principali contributori per avere un'idea generale della natura di un evento, ma usa AWS WAF i log per le tue decisioni di sicurezza. Per ulteriori informazioni, consultate le sezioni seguenti.

Le informazioni sugli eventi nella console Shield Advanced si basano sulle metriche di Shield Advanced. Per informazioni sulle metriche Shield Advanced, consulta AWS Shield Advanced metriche

I parametri di mitigazione non sono inclusi per le risorse CloudFront Amazon o Amazon Route 53, poiché questi servizi sono protetti da un sistema di mitigazione che è sempre abilitato e non richiede mitigazioni per singole risorse.

Le sezioni dei dettagli variano a seconda che le informazioni si riferiscano a un evento a livello di infrastruttura o a livello applicativo.

Dettagli degli eventi a livello di applicazione

Puoi visualizzare i dettagli sul rilevamento e la mitigazione di un evento a livello applicativo e sui principali contributori nella sezione inferiore della pagina della console relativa all'evento. Questa sezione può includere una combinazione di traffico legittimo e potenzialmente indesiderato e può rappresentare sia il traffico passato alla risorsa protetta sia il traffico bloccato dalle mitigazioni Shield Advanced.

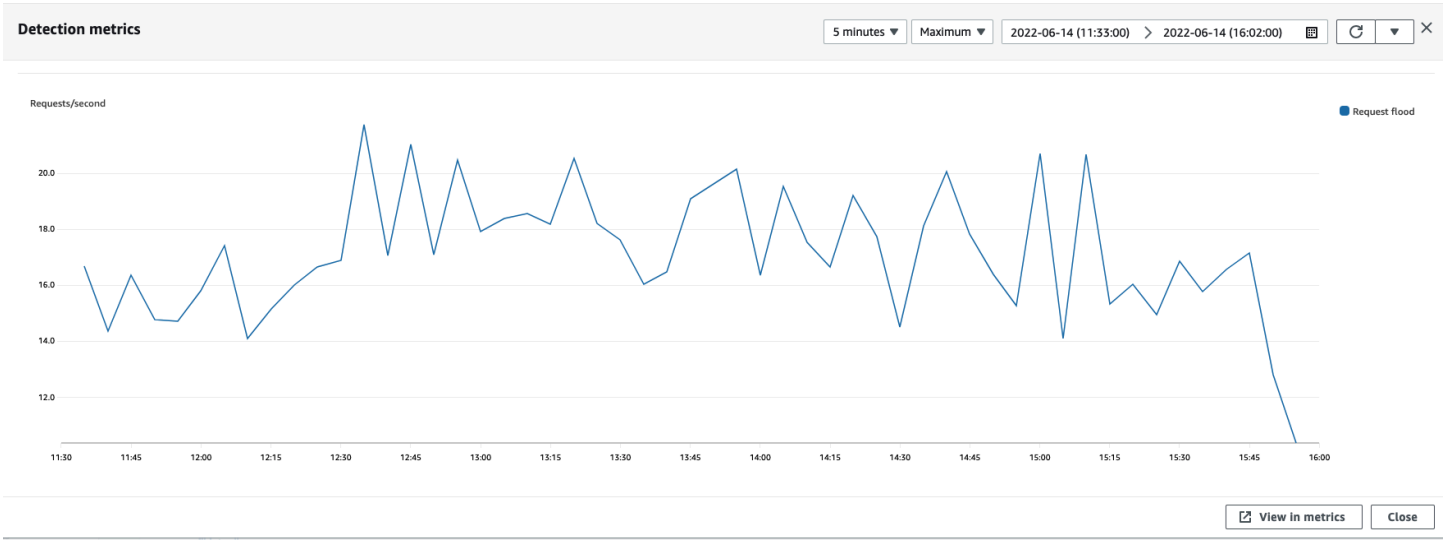
I dettagli di mitigazione riguardano tutte le regole dell'ACL Web associate alla risorsa, comprese le regole implementate specificamente in risposta a un attacco e le regole basate sulla frequenza definite nell'ACL Web. Se abiliti la mitigazione automatica degli attacchi DDoS a livello di applicazione per un'applicazione, le metriche di mitigazione includono le metriche per tali regole aggiuntive. Per informazioni su queste protezioni a livello di applicazione, consulta. AWS Shield Advanced protezioni a livello di applicazione (livello 7)

Rilevamento e mitigazione

Per un evento a livello applicativo (livello 7), la scheda Rilevamento e mitigazione mostra le metriche di rilevamento basate sulle informazioni ottenute dai log. AWS WAF Le metriche di mitigazione si basano su AWS WAF regole dell'ACL Web associato configurate per bloccare il traffico indesiderato.

Per CloudFront le distribuzioni Amazon, puoi configurare Shield Advanced per applicare mitigazioni automatiche al posto tuo. Con qualsiasi risorsa a livello di applicazione, puoi scegliere di definire le tue regole di mitigazione nell'ACL web e puoi richiedere assistenza allo Shield Response Team (SRT). Per informazioni su queste opzioni, consulta Risposta agli eventi DDoS.

La schermata seguente mostra un esempio delle metriche di rilevamento per un evento a livello applicativo che si è attenuato dopo alcune ore.



Il traffico degli eventi che diminuisce prima che una regola di mitigazione abbia effetto non è rappresentato nelle metriche di mitigazione. Ciò può comportare una differenza tra il traffico delle richieste Web mostrato nei grafici di rilevamento e le metriche di autorizzazione e blocco mostrate nei grafici di mitigazione.

Collaboratori principali

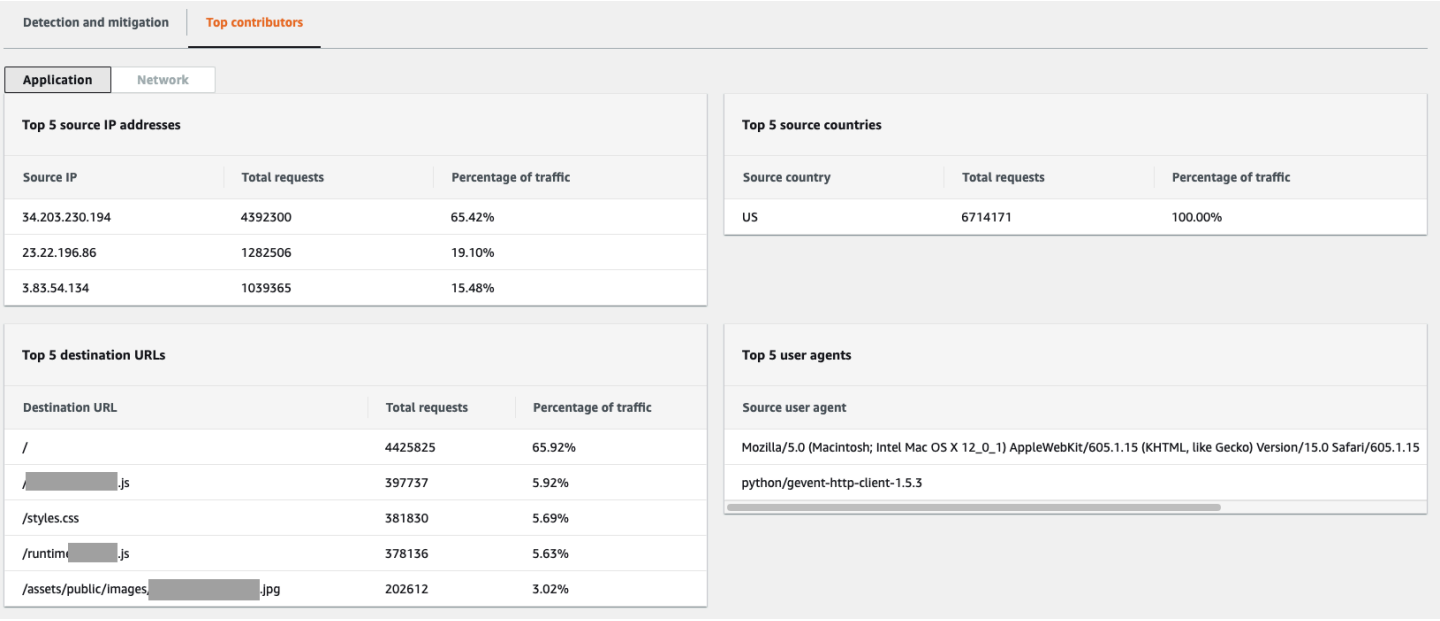
La scheda Collaboratori principali per gli eventi a livello di applicazione mostra i primi 5 contributori identificati da Shield per l'evento, in base AWS WAF ai log recuperati. Shield classifica le informazioni dei principali contributori in base a dimensioni quali IP di origine, paese di origine e URL di destinazione.

> **Note**
>
> Per informazioni più accurate sul traffico che contribuisce a un evento a livello di applicazione, utilizzate i AWS WAF log.

Utilizzate le informazioni sui principali contributori del livello di applicazione Shield solo per avere un'idea generale della natura di un attacco e non basate le vostre decisioni di sicurezza su di esso. Per gli eventi a livello di applicazione, AWS WAF i log sono la migliore fonte di informazioni per comprendere chi ha contribuito a un attacco e per elaborare strategie di mitigazione.

Le informazioni sui principali contributori di Shield non sempre riflettono completamente i dati nei AWS WAF log. Quando inserisce i log, Shield dà priorità alla riduzione dell'impatto sulle prestazioni del sistema rispetto al recupero del set completo di dati dai log. Ciò può comportare una perdita di granularità nei dati disponibili per l'analisi in Shield. Nella maggior parte dei casi, la maggior parte delle informazioni è disponibile, ma è possibile che i dati dei principali contributori vengano in qualche misura distorti a causa di qualsiasi attacco.

La schermata seguente mostra un esempio della scheda Top contributors per un evento a livello di applicazione.



Le informazioni sui contributori si basano sulle richieste di traffico legittimo e potenzialmente indesiderato. È più probabile che gli eventi con volume maggiore e gli eventi in cui le fonti delle richieste non sono distribuite in modo uniforme abbiano contributori principali identificabili. Un attacco distribuito in modo significativo può avere un numero qualsiasi di fonti, il che rende difficile identificare

i principali contributori all'attacco. Se Shield Advanced non identifica i contributori significativi per una categoria specifica, visualizza i dati come non disponibili.

Dettagli degli eventi a livello di infrastruttura

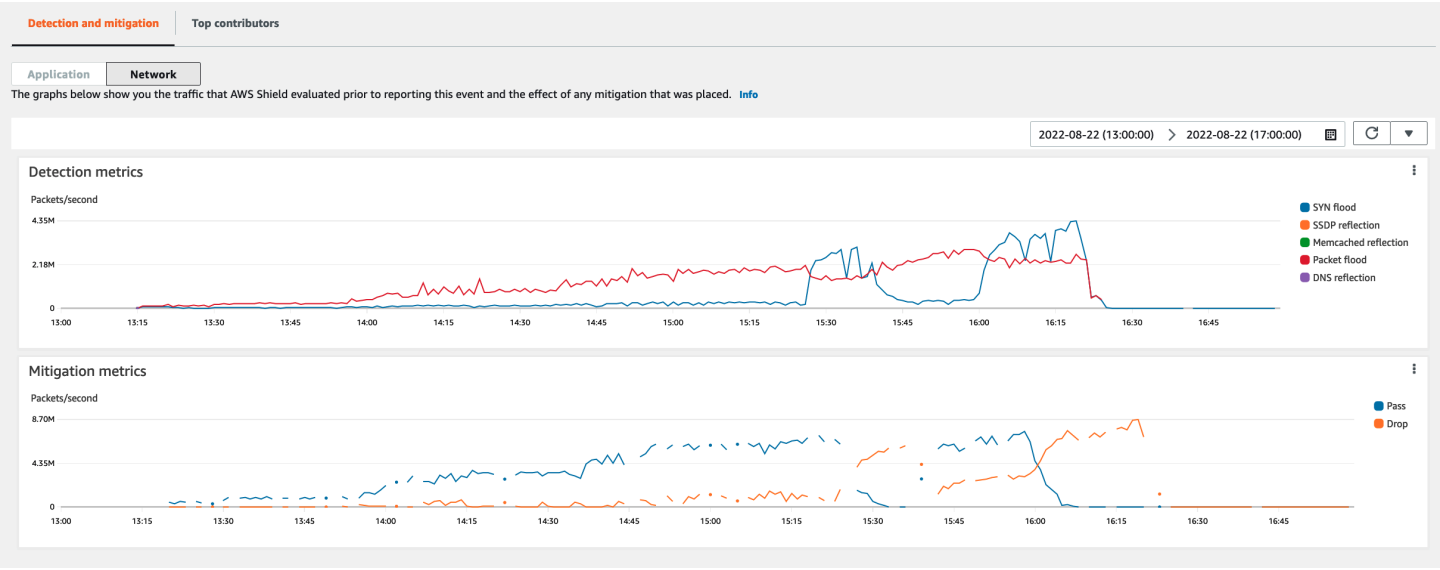
Puoi visualizzare i dettagli sul rilevamento e la mitigazione di un evento a livello di infrastruttura e sui principali contributori nella sezione inferiore della pagina della console relativa all'evento. Questa sezione può includere una combinazione di traffico legittimo e potenzialmente indesiderato e può rappresentare sia il traffico passato alla risorsa protetta sia il traffico bloccato dalle mitigazioni Shield.

Rilevamento e mitigazione

Per un evento a livello di infrastruttura (livello 3 o 4), la scheda Rilevamento e mitigazione mostra le metriche di rilevamento basate su flussi di rete campionati e le metriche di mitigazione basate sul traffico osservato dai sistemi di mitigazione. Le metriche di mitigazione sono una misurazione più precisa del traffico verso la risorsa.

Shield crea automaticamente una mitigazione per i tipi di risorse protette Elastic IP (EIP), Classic Load Balancer (CLB), Application Load Balancer (ALB) e acceleratore standard. AWS Global Accelerator Le metriche di mitigazione per gli indirizzi EIP e gli acceleratori AWS Global Accelerator standard indicano il numero di pacchetti passati e rilasciati.

La schermata seguente mostra un esempio di scheda Rilevamento e mitigazione per un evento a livello di infrastruttura.

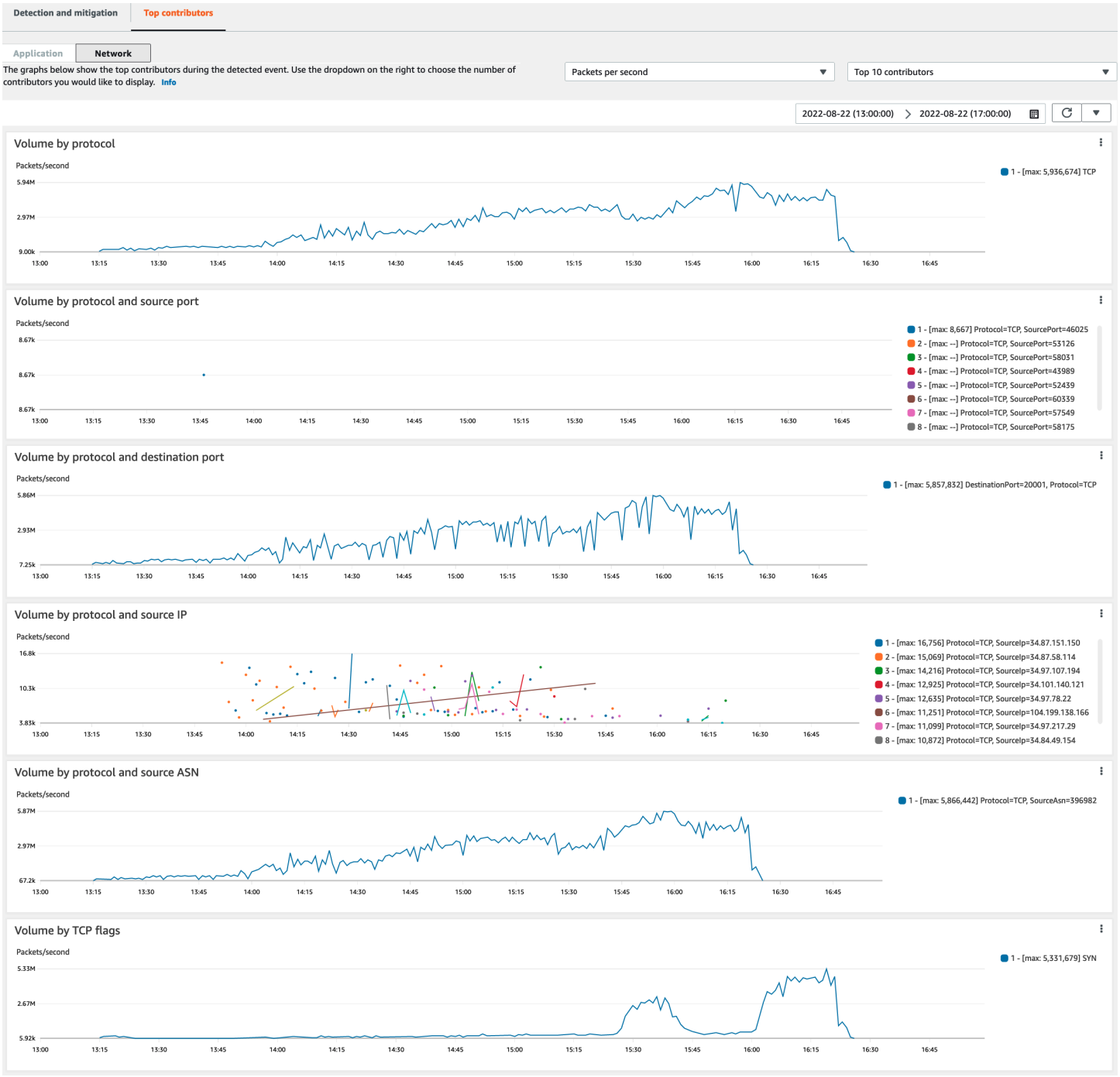


Il traffico degli eventi che si interrompe prima che Shield effettui una mitigazione non è rappresentato nelle metriche di mitigazione. Ciò può comportare una differenza tra il traffico mostrato nei grafici di rilevamento e le metriche relative al passaggio e alla caduta mostrate nei grafici di mitigazione.

Collaboratori principali

La scheda Collaboratori principali per gli eventi a livello di infrastruttura elenca le metriche relative a un massimo di 100 contributori principali in diverse dimensioni del traffico. I dettagli includono le proprietà del livello di rete per qualsiasi dimensione in cui è possibile identificare almeno cinque fonti di traffico significative. Esempi di fonti di traffico sono l'IP di origine e l'ASN di origine.

La schermata seguente mostra un esempio della scheda Top contributors per un evento a livello di infrastruttura.



Le metriche dei contributori si basano su flussi di rete campionati per il traffico legittimo e potenzialmente indesiderato. È più probabile che gli eventi con un volume maggiore e gli eventi in cui le fonti di traffico non sono distribuite in modo elevato abbiano contributori principali identificabili. Un attacco distribuito in modo significativo può avere un numero qualsiasi di fonti, il che rende difficile identificare i principali responsabili dell'attacco. Se Shield non identifica alcun contributore significativo per una metrica o una categoria specifica, visualizza i dati come non disponibili.

In un attacco DDoS a livello di infrastruttura, le sorgenti di traffico potrebbero essere falsificate o riflesse. Una fonte contraffatta viene falsificata intenzionalmente dall'aggressore. Una fonte riflessa è la vera fonte del traffico rilevato, ma non partecipa volontariamente all'attacco. Ad esempio, un utente malintenzionato potrebbe generare un flusso di traffico ampio e amplificato verso un bersaglio, riflettendo l'attacco su servizi su Internet che di solito sono legittimi. In questo caso, le informazioni sulla fonte potrebbero essere valide mentre non sono la fonte effettiva dell'attacco. Questi fattori possono limitare la fattibilità delle tecniche di mitigazione che bloccano le sorgenti in base alle intestazioni dei pacchetti.

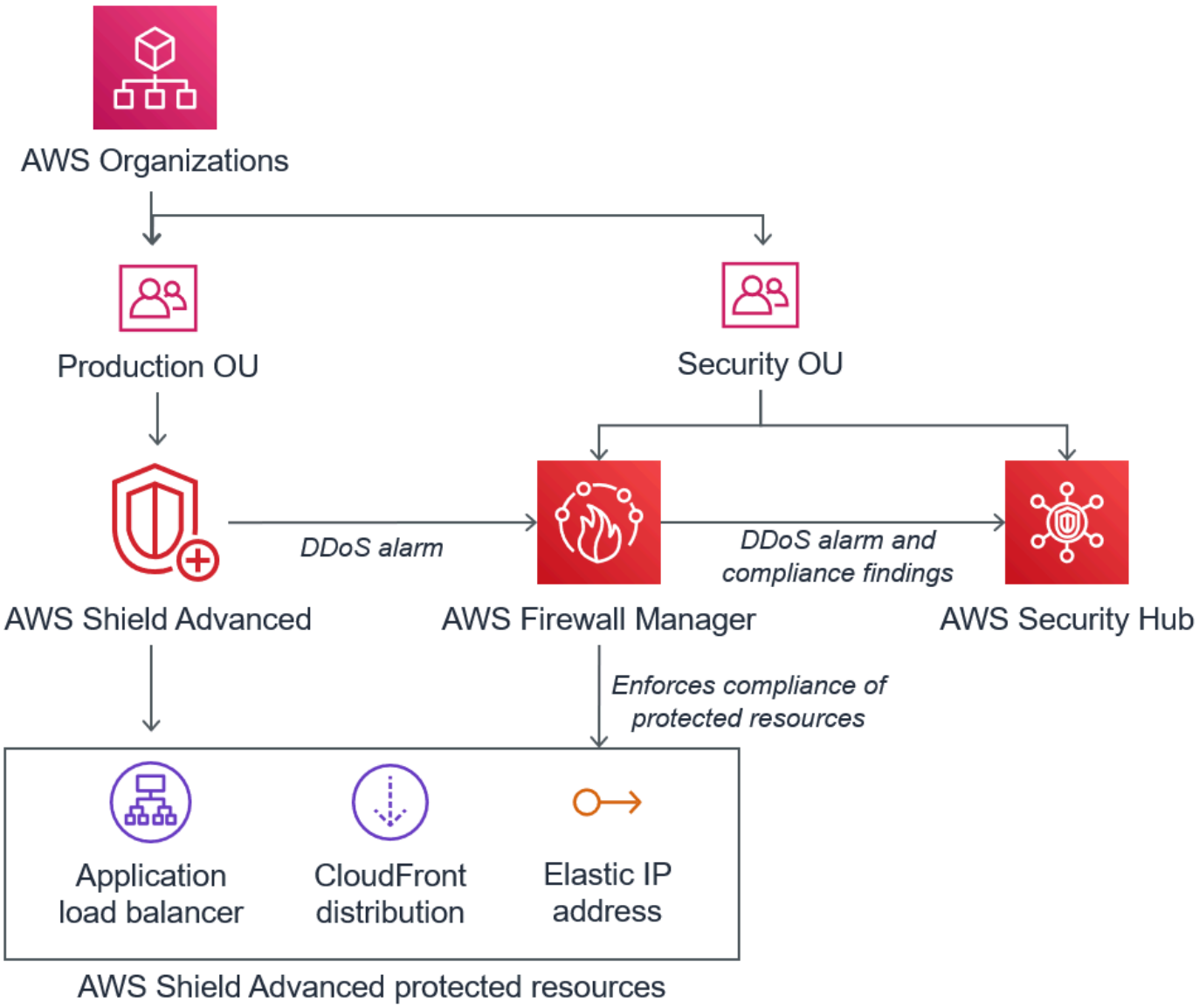
Visibilità degli eventi su tutti gli account

Puoi utilizzare, gestire AWS Firewall Manager e AWS Security Hub monitorare le risorse AWS Shield Advanced protette su più account.

Con Firewall Manager, puoi creare una politica di sicurezza Shield Advanced che riporta e applica la conformità alla protezione DDoS su tutti i tuoi account. Firewall Manager monitora le risorse protette, inclusa l'aggiunta di protezioni alle nuove risorse che rientrano nell'ambito della politica Shield Advanced.

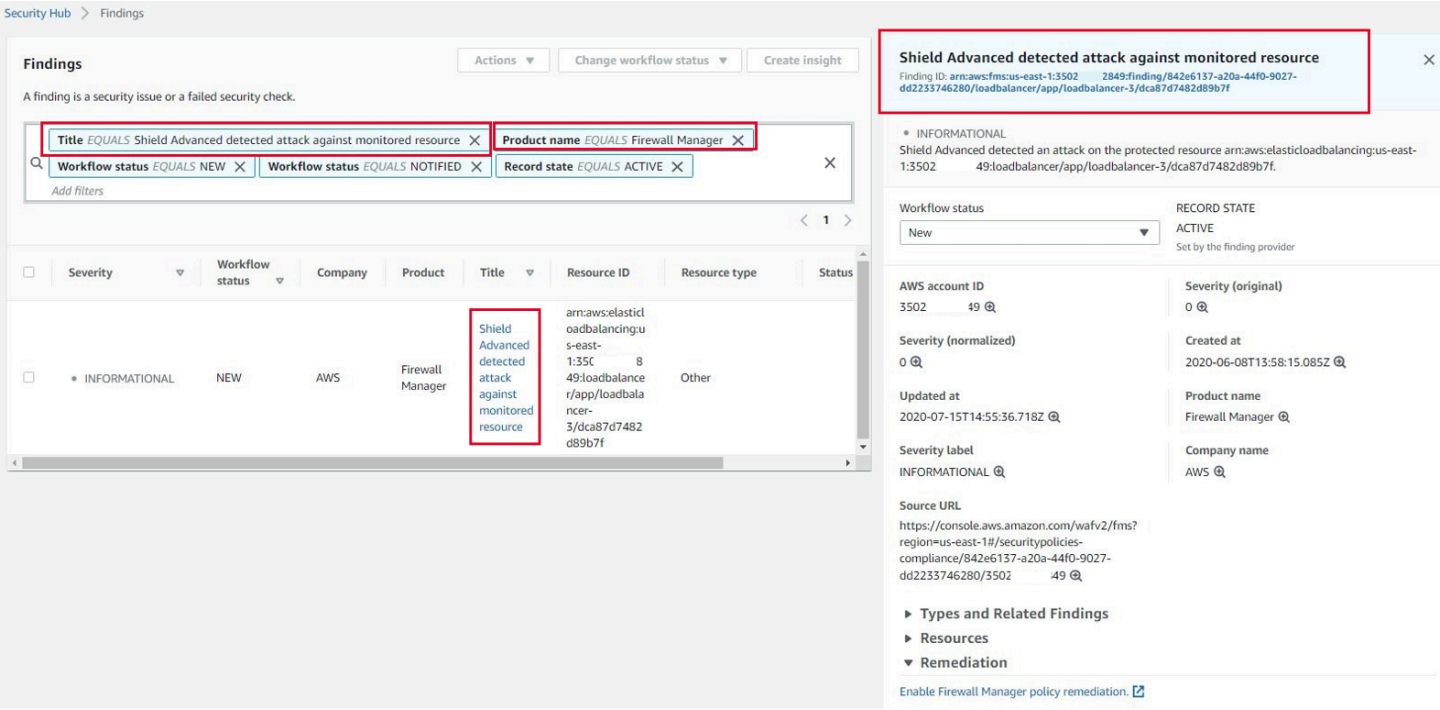
È possibile integrare Firewall Manager con AWS Security Hub per ottenere un'unica dashboard che riporti gli eventi DDoS rilevati dai risultati di conformità di Shield Advanced e Firewall Manager, quando Firewall Manager identifica una risorsa che non è conforme alla politica di sicurezza Shield Advanced.

La figura seguente illustra un'architettura tipica per il monitoraggio delle risorse protette Shield Advanced con Firewall Manager e Security Hub.



Quando integri Firewall Manager con Security Hub, puoi visualizzare i risultati di sicurezza in un unico posto, insieme ad altri avvisi e informazioni sullo stato di conformità per le applicazioni su AWS cui esegui.

La schermata seguente evidenzia le informazioni che è possibile visualizzare per un evento Shield Advanced all'interno della console Security Hub quando si dispone di un'integrazione di questo tipo.



Per scoprire come integrare Firewall Manager e Security Hub con Shield Advanced per centralizzare il monitoraggio degli eventi e della conformità tra gli account protetti, consulta il blog AWS sulla sicurezza Configurare il monitoraggio centralizzato degli eventi DDoS e correggere automaticamente le risorse non conformi.

Risposta agli eventi DDoS

AWS mitiga automaticamente gli attacchi DDoS (Distributed Denial of Service) a livello di rete e trasporto (livello 3 e livello 4). Se utilizzi Shield Advanced per proteggere le tue istanze Amazon EC2, durante un attacco Shield Advanced distribuisce automaticamente gli ACL di rete Amazon VPC al confine della rete. AWS Ciò consente a Shield Advanced di fornire protezione contro eventi DDoS di grandi dimensioni. Per ulteriori informazioni sulle liste di controllo degli accessi di rete, consulta l'articolo relativo alle liste di controllo degli accessi di rete.

Per gli attacchi DDoS a livello applicativo (livello 7), AWS i tentativi di rilevare e avvisare AWS Shield Advanced i clienti tramite CloudWatch allarmi. Per impostazione predefinita, non applica automaticamente le mitigazioni, per evitare di bloccare inavvertitamente il traffico utente valido.

Per le risorse a livello applicativo (livello 7), sono disponibili le seguenti opzioni per rispondere a un attacco.

- Fornisci le tue mitigazioni: puoi indagare e mitigare l'attacco da solo. Per informazioni, consulta Mitigazione manuale di un attacco DDoS a livello di applicazione.
- Contatta l'assistenza: se sei un cliente Shield Advanced, puoi contattare il AWS Support Centro per ricevere assistenza sulle mitigazioni. I casi critici e urgenti vengono trasmessi direttamente agli esperti DDoS. Per informazioni, consulta Contattare il centro di supporto durante un attacco DDoS a livello di applicazione.

Inoltre, prima che si verifichi un attacco, puoi abilitare in modo proattivo le seguenti opzioni di mitigazione:

- Attenuazioni automatiche sulle CloudFront distribuzioni Amazon: con questa opzione, Shield Advanced definisce e gestisce per te le regole di mitigazione nel tuo ACL web. Per informazioni sulla mitigazione automatica a livello di applicazione, consulta. Mitigazione DDoS automatica a livello di applicazione Shield Advanced
- Interazione proattiva: quando AWS Shield Advanced rileva un attacco a livello applicativo di grandi dimensioni contro una delle vostre applicazioni, SRT può contattarvi in modo proattivo. L'SRT valuta l'evento DDoS e crea mitigazioni. AWS WAF L'SRT ti contatta e, con il tuo consenso, può applicare le regole. AWS WAF Per ulteriori informazioni su questa opzione, consulta Configurazione del coinvolgimento proattivo.

Contattare il centro di supporto durante un attacco DDoS a livello di applicazione

Se sei un AWS Shield Advanced cliente, puoi contattare il AWS Support Centro per ricevere assistenza sulle mitigazioni. I casi critici e urgenti vengono trasmessi direttamente agli esperti DDoS. Inoltre AWS Shield Advanced, i casi complessi possono essere inoltrati allo AWS Shield Response Team (SRT), che ha una vasta esperienza nella protezione AWS, ad Amazon.com e alle sue filiali. Per ulteriori informazioni sull'SRT, consulta. Supporto dello Shield Response Team (SRT)

Per ricevere assistenza dallo Shield Response Team (SRT), contatta il AWS Support Centro. Il tempo di risposta per il tuo caso dipende dalla gravità selezionata e dai tempi di risposta, documentati nella pagina AWS Support Piani.

Selezionare le seguenti opzioni:

- Tipo di caso: Supporto tecnico
- Servizio: Distributed Denial of Service (DDoS)

- Categoria: In arrivo verso AWS
- Gravità: Scegliere un'opzione appropriata

Quando parli con il nostro rappresentante, spiega che sei un AWS Shield Advanced cliente che sta subendo un possibile attacco DDoS. Il nostro rappresentante girerà la chiamata agli esperti DDoS adatti. Se apri un caso con il AWS Support Centro utilizzando il tipo di servizio Distributed Denial of Service (DDoS), puoi parlare direttamente con un esperto di DDoS tramite chat o telefono. I tecnici dell'assistenza DDoS possono aiutarti a identificare gli attacchi, consigliare miglioramenti all' AWS architettura e fornire indicazioni sull'uso dei AWS servizi per la mitigazione degli attacchi DDoS.

Per gli attacchi a livello applicativo, l'SRT può aiutarvi ad analizzare le attività sospette. Se hai abilitato la mitigazione automatica per la tua risorsa, l'SRT può esaminare le mitigazioni che Shield Advanced sta implementando automaticamente contro l'attacco. In ogni caso, l'SRT può aiutarvi a esaminare e mitigare il problema. Le mitigazioni consigliate dall'SRT spesso richiedono all'SRT di creare o aggiornare elenchi di controllo degli accessi AWS WAF Web (ACL Web) nell'account. L'SRT avrà bisogno della tua autorizzazione per eseguire questo lavoro.

> **Important**
>
> Come parte dell'attivazione AWS Shield Advanced, ti consigliamo di seguire i passaggi indicati per fornire in modo proattivo Configurazione dell'accesso per lo Shield Response Team (SRT) all'SRT le autorizzazioni di cui ha bisogno per assisterti durante un attacco. Concedere in anticipo l'autorizzazione consente di evitare ritardi in caso di attacco imminente.

L'SRT ti aiuta a classificare l'attacco DDoS per identificare le firme e i modelli di attacco. Con il tuo consenso, l'SRT crea e AWS WAF implementa regole per mitigare l'attacco.

Puoi anche contattare l'SRT prima o durante un possibile attacco per esaminare le mitigazioni e sviluppare e implementare mitigazioni personalizzate. Ad esempio, se state eseguendo un'applicazione Web e avete bisogno di aprire solo le porte 80 e 443, potete lavorare con SRT per preconfigurare un ACL web in modo che «consenta» solo le porte 80 e 443.

Autorizzi e contatti l'SRT a livello di account. Cioè, se si utilizza Shield Advanced all'interno di una politica Firewall Manager Shield Advanced, il proprietario dell'account, non l'amministratore di Firewall Manager, deve contattare SRT per ricevere assistenza. L'amministratore di Firewall Manager può contattare SRT solo per gli account di sua proprietà.

Mitigazione manuale di un attacco DDoS a livello di applicazione

Se stabilisci che l'attività nella pagina degli eventi relativa alla tua risorsa rappresenta un attacco DDoS, puoi creare AWS WAF regole personalizzate nell'ACL web per mitigare l'attacco. Questa è l'unica opzione disponibile se non sei un cliente Shield Advanced. AWS WAF è inclusa senza AWS Shield Advanced costi aggiuntivi. Per informazioni sulla creazione di regole nell'ACL Web, consultaElenchi di controllo degli accessi Web (ACL Web).

Se lo utilizzi AWS Firewall Manager, puoi aggiungere AWS WAF le tue regole a una AWS WAF politica di Firewall Manager.

Per mitigare manualmente un potenziale attacco DDoS a livello applicativo

1. Crea istruzioni di regole nell'ACL web con criteri che corrispondono al comportamento insolito. Per cominciare, configurali per contare le richieste corrispondenti. Per informazioni sulla configurazione dell'ACL Web e delle istruzioni delle regole, consulta Valutazione delle regole ACL Web e dei gruppi di regole e. Test e ottimizzazione delle protezioni AWS WAF

   > **Note**
   >
   > Verifica sempre prima le tue regole utilizzando inizialmente l'azione della regola Count anziché. Block Dopo aver verificato che le nuove regole identificano le richieste corrette, puoi modificarle per bloccarle.

2. Monitora il conteggio delle richieste per determinare se desideri bloccare le richieste corrispondenti. Se il volume delle richieste continua a essere insolitamente elevato e sei sicuro che le tue regole stiano catturando le richieste che stanno causando l'elevato volume, modifica le regole dell'ACL web per bloccare le richieste.
3. Continua a monitorare la pagina degli eventi per assicurarti che il traffico venga gestito come desideri.

AWS fornisce modelli preconfigurati per iniziare rapidamente. I modelli includono una serie di AWS WAF regole che puoi personalizzare e utilizzare per bloccare gli attacchi più comuni basati sul Web. Per ulteriori informazioni, consulta l'articolo relativo alle automazioni di sicurezza AWS WAF.

Richiedere un credito in AWS Shield Advanced

Se sei abbonato AWS Shield Advanced e subisci un attacco DDoS che aumenta l'utilizzo di una risorsa protetta Shield Advanced, puoi richiedere un credito per il servizio Shield Advanced per gli addebiti relativi al maggiore utilizzo, nella misura in cui questo non sia mitigato da Shield Advanced.

I crediti sono disponibili solo per i seguenti tipi di addebiti:

- Uscita dati Shield Advanced
- Richieste Amazon CloudFront HTTP/HTTPS
- CloudFront trasferimento dati in uscita
- Interrogazioni su Amazon Route 53
- AWS Global Accelerator trasferimento dati con acceleratore standard
- Unità di capacità di bilanciamento del carico per Application Load Balancer
- Costi delle istanze per le istanze protette di Amazon Elastic Compute Cloud (Amazon EC2) create da una politica di auto-scaling in risposta all'attacco

Prerequisiti per richiedere un credito

Per avere diritto a ricevere un credito, prima dell'inizio dell'attacco, devi aver fatto quanto segue:

- È necessario aver aggiunto la protezione Shield Advanced alle risorse per le quali si desidera richiedere un credito. Le risorse protette aggiunte durante un attacco non sono idonee alla protezione dei costi.

  > **Note**
  >
  > L'attivazione di Shield Advanced sul tuo Account AWS non abilita automaticamente la protezione Shield Advanced per le singole risorse.

  Per ulteriori informazioni su come proteggere AWS le risorse utilizzando Shield Advanced, vedereAggiungere AWS Shield Advanced protezione alle risorse AWS.
- Per le risorse applicabili CloudFront e protette da Application Load Balancer, è necessario aver associato un ACL AWS WAF Web e implementato una regola basata sulla velocità nell'ACL Web in modalità. Block Per informazioni sulle regole basate sulla AWS WAF velocità, vedere. Istruzione

regola basata sulla frequenza Per informazioni su come associare gli ACL Web alle AWS risorse, vedere. Elenchi di controllo degli accessi Web (ACL Web)

- È necessario aver implementato le migliori pratiche appropriate nelle AWS Best Practices for DDoS Resiliency per configurare l'applicazione in modo da ridurre al minimo i costi durante un attacco DDoS.

Come richiedere un credito

Per avere diritto a un credito, è necessario inviare la richiesta di credito entro il periodo di 15 giorni immediatamente successivo al mese di fatturazione in cui si è verificato l'attacco.

Per richiedere un credito, invia una richiesta di fatturazione tramite il AWS Support Centro. Includi quanto segue nella tua richiesta:

- Le parole "DDoS Concession" nell'oggetto
- Le date e gli orari di ogni evento o interruzione della disponibilità per cui richiedi un credito
- I AWS servizi e le risorse specifiche interessati

Dopo aver inviato una richiesta, lo AWS Shield Response Team (SRT) verificherà se si è verificato un attacco DDoS e, in caso affermativo, se le risorse protette sono state ridimensionate per assorbire l'attacco DDoS. Se AWS determina che le risorse protette sono state ridimensionate per assorbire l'attacco DDoS, AWS emetterà un credito per la parte di traffico che AWS ritiene sia stata causata dall'attacco DDoS. I crediti sono validi per 12 mesi.

Sicurezza nell'utilizzo del AWS Shield servizio

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

> **Note**
>
> Questa sezione fornisce linee guida AWS di sicurezza standard per l'utilizzo del AWS Shield servizio e delle sue AWS risorse, come le protezioni Shield Advanced.
> Per informazioni sulla protezione AWS delle risorse utilizzando Shield e Shield Advanced, consulta il resto della AWS Shield guida.

La sicurezza è una responsabilità condivisa tra te AWS e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. L'efficacia della nostra sicurezza è regolarmente testata e verificata da revisori di terze parti come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità che si applicano a Shield, consulta AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e leggi e normative applicabili.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza Shield. Negli argomenti seguenti viene illustrato come configurare Shield per soddisfare gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Shield.

Argomenti

Protezione dei dati in Shield

Il modello di responsabilità AWS di si applica alla protezione dei dati in AWS Shield. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Shield o altro Servizi AWS utilizzando la console, l'API o AWS gli SDK. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Le entità Shield, come le protezioni, sono crittografate a riposo, tranne in alcune regioni in cui la crittografia non è disponibile, tra cui Cina (Pechino) e Cina (Ningxia). Per ogni regione vengono utilizzate chiavi di crittografia univoche.

Gestione delle identità e degli accessi per AWS Shield

AWS Identity and Access Management (IAM) aiuta un Servizio AWS amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (dispone delle autorizzazioni) a utilizzare le risorse Shield. IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Shield.

Utente del servizio: se utilizzi il servizio Shield per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità Shield per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Shield, consultaRisoluzione dei problemi di AWS Shield identità e accesso.

Amministratore del servizio: se sei responsabile delle risorse Shield della tua azienda, probabilmente hai pieno accesso a Shield. È tuo compito determinare a quali funzionalità e risorse Shield devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con Shield, consultaCome AWS Shield funziona con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso a Shield. Per visualizzare esempi di policy basate sull'identità Shield che puoi utilizzare in IAM, consulta. Esempi di policy basate su identità per AWS Shield

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per

ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM

può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'azione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruoli IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per sapere come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come AWS Shield funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a Shield, scopri quali funzionalità IAM sono disponibili per l'uso con Shield.

Funzionalità IAM che puoi utilizzare con AWS Shield

Funzionalità IAM	Supporto Shield
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come Shield e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per Shield

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Per visualizzare esempi di politiche basate sull'identità di Shield, vedere. Esempi di policy basate su identità per AWS Shield

Politiche basate sulle risorse all'interno di Shield

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una

policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Azioni politiche per Shield

Supporta le azioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni Shield, vedere Azioni definite da AWS Shield nel Service Authorization Reference.

Le azioni politiche in Shield utilizzano il seguente prefisso prima dell'azione:

```
shield
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "shield:action1",
      "shield:action2"
         ]
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni in Shield che iniziano con`List`, includi la seguente azione:

```
"Action": "shield:List*"
```

Per visualizzare esempi di politiche basate sull'identità di Shield, vedere. Esempi di policy basate su identità per AWS Shield

Risorse politiche per Shield

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare l'elenco dei tipi di risorse Shield e dei relativi ARN, vedere Resources defined by AWS Shield nel Service Authorization Reference. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta la sezione Operazioni definite da AWS Shield. Per consentire o negare l'accesso a un sottoinsieme di risorse Shield, includi l'ARN della risorsa nell'`resource`elemento della tua politica.

Nel AWS Shield, le risorse sono protezioni e attacchi. Alle risorse sono associati nomi Amazon Resource Name (ARN) univoci, come illustrato nella tabella seguente.

Nome nella console AWS Shield	Nome in AWS Shield SDK/ CLI	Formato ARN	
Evento o attacco	`AttackDetail`	`arn:aws:shield:: account:attack/ID`	

Nome nella console AWS Shield	Nome in AWS Shield SDK/ CLI	Formato ARN
Protezione	`Protection`	`arn:aws:shield:: account:protection/ ID`

Per consentire o negare l'accesso a un sottoinsieme di risorse Shield, includi l'ARN della risorsa nell'`resource`elemento della tua politica. Gli ARN per Shield hanno il seguente formato:

```
arn:partition:shield::account:resource/ID
```

Sostituisci le variabili *`account`*, *`resource`* e *`ID`* con valori validi. I valori validi possono essere i seguenti:

- *`account`*: l'ID del tuo Account AWS. È necessario specificare un valore.
- *`risorsa`*: il tipo di risorsa Shield, `attack` oppure`protection`.
- *`ID`*: l'ID della risorsa Shield o un carattere jolly (`*`) per indicare tutte le risorse del tipo specificato associate alla risorsa specificata Account AWS.

Ad esempio, il seguente ARN specifica tutte le protezioni per l'account `111122223333`:

```
arn:aws:shield::111122223333:protection/*
```

Le risorse ARN of Shield hanno il seguente formato:

```
arn:partition:shield:region:account-id:scope/resource-type/resource-name/resource-id
```

Per informazioni generali sulle specifiche ARN, consulta Amazon Resource Names (ARNs) nel. Riferimenti generali di Amazon Web Services

Di seguito sono elencati i requisiti specifici degli ARN delle risorse: `wafv2`

- *`regione`*: Per le risorse Shield che usi per proteggere CloudFront le distribuzioni Amazon, imposta questa opzione su. `us-east-1` Altrimenti, impostala sulla regione che stai utilizzando con le tue risorse regionali protette.

- *ambito*: imposta l'ambito `global` per l'utilizzo con una CloudFront distribuzione Amazon o `regional` per l'utilizzo con una qualsiasi delle risorse regionali AWS WAF supportate. Le risorse regionali sono un'API REST di Amazon API Gateway, un'Application Load Balancer, un'API GraphQL AWS AppSync , un pool di utenti Amazon Cognito, un AWS App Runner servizio e un'istanza Verified Access. AWS
- *tipo di risorsa*: specifica uno dei seguenti valori: `attack` per eventi o attacchi, per protezioni. `protection`
- *resource-name*: specificate il nome che avete assegnato alla risorsa Shield o specificate un wildcard (`*`) per indicare tutte le risorse che soddisfano le altre specifiche dell'ARN. È necessario specificare il nome e l'ID della risorsa o specificare un carattere jolly per entrambi.
- *resource-id*: Specificate l'ID della risorsa Shield o specificate un wildcard (`*`) per indicare tutte le risorse che soddisfano le altre specifiche dell'ARN. È necessario specificare il nome e l'ID della risorsa o specificare un carattere jolly per entrambi.

Ad esempio, il seguente ARN specifica tutte le ACL Web con ambito regionale per l'account `111122223333` nella regione `us-west-1`:

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

Il seguente ARN specifica il gruppo di regole denominato `MyIPManagementRuleGroup` con ambito globale per l'account `111122223333` in Region: `us-east-1`

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

Per visualizzare esempi di politiche basate sull'identità di Shield, vedere. Esempi di policy basate su identità per AWS Shield

Chiavi relative alle condizioni delle policy per Shield

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco delle chiavi di condizione Shield, vedere Condition keys for AWS Shield nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, vedi Azioni definite da AWS Shield.

Per visualizzare esempi di politiche basate sull'identità di Shield, vedere. Esempi di policy basate su identità per AWS Shield

ACL in Shield

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con Shield

Supporta ABAC (tag nelle policy)	Parziale

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Shield

Supporta le credenziali temporanee	Sì

Alcune Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare

dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Sessioni di accesso diretto per Shield

Supporta sessioni di accesso diretto (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

Ruoli di servizio per Shield

Supporta i ruoli di servizio	Sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità Shield. Modifica i ruoli di servizio solo quando Shield fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per Shield

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione dei ruoli collegati ai servizi Shield, vedere. Utilizzo di ruoli collegati ai servizi per Shield Advanced

Esempi di policy basate su identità per AWS Shield

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare le risorse Shield. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS l'API. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da Shield, incluso il formato degli ARN per ciascun tipo di risorsa, vedere Azioni, risorse e chiavi di condizione AWS Shield nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console Shield
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Concedi l'accesso in lettura alle tue protezioni Shield Advanced
- Concedi l'accesso in sola lettura a Shield e CloudFront CloudWatch
- Concedi l'accesso completo a Shield CloudFront, e CloudWatch

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse Shield nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso ad azioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Shield

Per accedere alla AWS Shield console, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse Shield

presenti nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Gli utenti che possono accedere e utilizzare la AWS console possono accedere anche alla AWS Shield console. Non sono necessarie autorizzazioni supplementari.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o a livello di codice utilizzando l' AWS CLI API 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": "*"
        }
    ]
}
```

Concedi l'accesso in lettura alle tue protezioni Shield Advanced

AWS Shield consente l'accesso alle risorse tra account, ma non consente di creare protezioni delle risorse tra account. È possibile creare protezioni per le risorse solo dall'interno dell'account proprietario di tali risorse.

Di seguito viene riportata una policy di esempio che concede le autorizzazioni per l'operazione `shield:ListProtections` su tutte le risorse. Shield non supporta l'identificazione di risorse specifiche utilizzando gli ARN delle risorse (denominati anche autorizzazioni a livello di risorsa) per alcune azioni dell'API, quindi è necessario specificare un carattere jolly (*). Ciò consente l'accesso solo alle risorse che è possibile recuperare tramite l'azione. `ListProtections`

```
{
    "Version": "2016-06-02",
    "Statement": [
        {
            "Sid": "ListProtections",
            "Effect": "Allow",
            "Action": [
                "shield:ListProtections"
            ],
            "Resource": "*"
        }
    ]
}
```

Concedi l'accesso in sola lettura a Shield e CloudFront CloudWatch

La seguente politica garantisce agli utenti l'accesso in sola lettura a Shield e alle risorse associate, incluse le CloudFront risorse Amazon e i parametri Amazon. CloudWatch È utile per gli utenti che necessitano dell'autorizzazione per visualizzare le impostazioni nelle protezioni e negli attacchi Shield e per monitorare le metriche in. CloudWatch Questi utenti non possono creare, aggiornare o eliminare le risorse 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": "*"
            }
    ]
}
```

Concedi l'accesso completo a Shield CloudFront, e CloudWatch

La seguente politica consente agli utenti di eseguire qualsiasi operazione Shield, eseguire qualsiasi operazione sulle distribuzioni CloudFront Web e monitorare le metriche e un campione di richieste in. CloudWatch È utile per gli utenti che sono amministratori di 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": "*"
            }
      ]
```

```
}
```

Consigliamo vivamente di configurare l'autenticazione a più fattori (MFA) per gli utenti che dispongono di autorizzazioni amministrative. Per ulteriori informazioni, consulta Using Multi-Factor Authentication (MFA) Devices AWS with nella IAM User Guide.

AWS politiche gestite per AWS Shield

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AWS politica gestita: AWSShieldDRTAccessPolicy

AWS Shield utilizza questa politica gestita quando concedi l'autorizzazione allo Shield Response Team (SRT) di agire per tuo conto. Questa politica offre all'SRT un accesso limitato al vostro AWS account, per aiutarvi a mitigare gli attacchi DDoS durante eventi ad alta gravità. Questa politica consente a SRT di gestire AWS WAF le regole e le protezioni Shield Advanced e di accedere AWS WAF ai registri.

Per informazioni sulla concessione dell'autorizzazione all'SRT di operare per vostro conto, consultate. Configurazione dell'accesso per lo Shield Response Team (SRT)

Per i dettagli su questa politica, consulta AWSShieldDRTAccessPolicynella console IAM.

AWS politica gestita: AWSShieldServiceRolePolicy

Shield Advanced utilizza questa politica gestita quando abiliti la mitigazione automatica degli attacchi DDoS a livello di applicazione, per impostare le autorizzazioni necessarie per gestire le risorse del tuo account. Questa politica consente a Shield Advanced di creare e applicare AWS WAF regole e gruppi di regole negli ACL Web associati alle risorse protette, per rispondere automaticamente agli attacchi DDoS.

Non puoi collegarti AWSShieldServiceRolePolicy alle tue entità IAM. Shield associa questa politica al ruolo collegato al servizio per `AWSServiceRoleForAWSShield` consentire a Shield di eseguire azioni per conto dell'utente.

Shield Advanced consente l'uso di questa policy quando si abilita la mitigazione automatica degli attacchi DDoS a livello di applicazione. Per ulteriori informazioni sull'utilizzo di questa politica, vedere. Mitigazione DDoS automatica a livello di applicazione Shield Advanced

Per informazioni sul ruolo collegato al servizio AWSServiceRoleForAWSShield che utilizza questa politica, consulta Utilizzo di ruoli collegati ai servizi per Shield Advanced

Per i dettagli su questa politica, consulta AWSShieldServiceRolePolicynella console IAM.

Aggiornamenti Shield alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Shield da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei documenti Shield all'indirizzo. Cronologia dei documenti

Policy	Descrizione della modifica	Data
`AWSShieldServiceRolePolicy` Questa politica consente a Shield di accedere e gestire AWS le risorse per rispondere automaticamente agli attacchi	È stato aggiunto questo criterio per fornire a Shield Advanced le autorizzazioni necessarie per la funzionalità di mitigazione degli attacchi DDoS a livello di applicazi one automatica. Per informazi oni su questa funzional	1° dicembre 2021

Policy	Descrizione della modifica	Data
DDoS a livello di applicazione per tuo conto. Dettagli nella console IAM: AWSShieldServiceRolePolicy Il ruolo collegato al servizio `AWSServiceRoleForAWSShield` utilizza questa politica. Per informazioni, consulta Utilizzo di ruoli collegati ai servizi per Shield Advanced.	ità, consulta. Mitigazione DDoS automatica a livello di applicazione Shield Advanced	
Shield ha iniziato a tracciare le modifiche	Shield ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	3 marzo 2021

Risoluzione dei problemi di AWS Shield identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Shield e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in Shield
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Shield

Non sono autorizzato a eseguire un'azione in Shield

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `shield:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 shield:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `shield:GetWidget`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo a Shield.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Shield. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Shield

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Shield supporta queste funzionalità, consultaCome AWS Shield funziona con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Utilizzo di ruoli collegati ai servizi per Shield Advanced

AWS Shield Advanced utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a Shield Advanced. I ruoli collegati ai servizi sono predefiniti da Shield Advanced e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per tuo conto.

Un ruolo collegato al servizio semplifica la configurazione di Shield Advanced perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Shield Advanced definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo Shield Advanced può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. In questo modo proteggi le tue risorse Shield Advanced perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per Shield Advanced

Shield Advanced utilizza il ruolo collegato al servizio denominato. AWSServiceRoleForAWSShield Questo ruolo consente a Shield Advanced di accedere e gestire AWS le risorse per rispondere automaticamente agli attacchi DDoS a livello di applicazione per tuo conto. Per ulteriori informazioni su questa funzionalità, vedereMitigazione DDoS automatica a livello di applicazione Shield Advanced.

Il ruolo AWSServiceRoleForAWSShield collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `shield.amazonaws.com`

La politica di autorizzazione dei ruoli denominata AWSShieldServiceRolePolicy consente a Shield Advanced di completare le seguenti azioni su tutte le AWS risorse:

- `wafv2:GetWebACL`
- `wafv2:UpdateWebACL`
- `wafv2:GetWebACLForResource`
- `wafv2:ListResourcesForWebACL`
- `cloudfront:ListDistributions`
- `cloudfront:GetDistribution`

Quando le azioni sono consentite su tutte AWS le risorse, ciò è indicato nella politica come`"Resource": "*"`. Ciò significa solo che il ruolo collegato al servizio può eseguire ogni azione indicata su tutte le AWS risorse supportate dall'azione. Ad esempio, l'azione `wafv2:GetWebACL` è supportata solo per le risorse `wafv2` Web ACL.

Shield Advanced effettua chiamate API a livello di risorsa solo per le risorse protette per le quali hai abilitato la funzionalità di protezione a livello di applicazione e per gli ACL Web associati a tali risorse protette.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Shield Advanced

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando abiliti la mitigazione automatica degli attacchi DDoS a livello di applicazione per una risorsa nella AWS Management Console, nella o nell' AWS API AWS CLI, Shield Advanced crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando abiliti la mitigazione automatica degli attacchi DDoS a livello di applicazione per una risorsa, Shield Advanced crea nuovamente il ruolo collegato al servizio per te.

Modifica di un ruolo collegato ai servizi per Shield Advanced

Shield Advanced non consente di modificare il ruolo AWSServiceRoleForAWSShield collegato al servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Shield Advanced

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

> **Note**
>
> Se Shield Advanced utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse Shield Advanced utilizzate da AWSServiceRoleForAWSShield

Per tutte le risorse su cui sono configurate le protezioni DDoS a livello di applicazione, disabilita la mitigazione automatica degli attacchi DDoS a livello di applicazione. Per le istruzioni sulla console, vedere. Configura le protezioni DDoS a livello di applicazione

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo AWSServiceRoleForAWSShield collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi Shield Advanced

Shield Advanced supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Endpoint e quote Shield Advanced.

Registrazione e monitoraggio in Shield

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Shield e delle tue AWS soluzioni. È necessario raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. AWS fornisce diversi strumenti per monitorare le risorse Shield e rispondere a potenziali eventi:

CloudWatch Allarmi Amazon

Utilizzando gli CloudWatch allarmi, controlli una singola metrica per un periodo di tempo specificato. Se la metrica supera una determinata soglia, CloudWatch invia una notifica a un argomento o una policy di Amazon SNS. AWS Auto Scaling Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch.

AWS CloudTrail Registri

CloudTrail fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Shield. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a Shield, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi. Per ulteriori informazioni, consulta Registrazione delle chiamate API di AWS CloudTrail con.

Convalida della conformità per Shield

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

  > **Note**
  >
  > Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e

verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.

- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente AWS l'utilizzo per semplificare la gestione dei rischi e la conformità alle normative e agli standard di settore.

Resilienza in Shield

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

Sicurezza dell'infrastruttura nell' AWS Shield

In quanto servizio gestito, AWS Shield è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere a Shield attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

AWS Shield Advanced quote

AWS Shield Advanced ha quote predefinite sul numero di entità per regione. È possibile richiedere un aumento di queste quote.

Risorsa	Quota predefinita
Numero massimo di risorse protette per ogni tipo di risorsa che AWS Shield Advanced offre protezione, per account.	1.000
Numero massimo di gruppi di protezione, per account.	100
Numero massimo di singole risorse protette che è possibile includere in modo specifico in un gruppo di protezione. Nell'API, questo si applica a `Members` quello specificato quando si imposta il gruppo di protezione `Pattern` su`ARBITRARY` . Nella console, ciò si applica alle risorse selezionate per il gruppo di protezione Scegli tra risorse protette.	1.000

AWS Firewall Manager

AWS Firewall Manager semplifica le attività di amministrazione e manutenzione su più account e risorse per una varietà di protezioni AWS WAF, tra cui gruppi di sicurezza AWS Shield Advanced Amazon VPC AWS Network Firewall e Amazon Route 53 Resolver DNS Firewall. Con Firewall Manager, le protezioni vengono configurate una sola volta e il servizio le applica automaticamente a tutti gli account e le risorse, anche quando si aggiungono nuovi account e risorse.

Firewall Manager fornisce i seguenti vantaggi:

- Consente di proteggere le risorse su tutti gli account
- Aiuta a proteggere tutte le risorse di un tipo particolare, come tutte le CloudFront distribuzioni Amazon
- Consente di proteggere tutte le risorse con tag specifici
- Consente di aggiungere automaticamente la protezione per le risorse aggiunte all'account
- Consente di sottoscrivere tutti gli account dei membri di un' AWS Organizations organizzazione e sottoscrive automaticamente i nuovi account pertinenti che entrano a far AWS Shield Advanced parte dell'organizzazione
- Consente di applicare regole di gruppo di protezione a tutti gli account membri o sottoinsiemi specifici di account in un'organizzazione AWS Organizations e di applicare automaticamente le regole ai nuovi account che entrano a far parte dell'organizzazione
- Consente di utilizzare regole personalizzate o acquistare regole gestite da Marketplace AWS

Firewall Manager è particolarmente utile quando si desidera proteggere l'intera organizzazione anziché un numero limitato di account e risorse specifici o se si aggiungono frequentemente nuove risorse da proteggere. Firewall Manager fornisce anche il monitoraggio centralizzato degli attacchi DDoS all'interno dell'organizzazione.

Argomenti

- Utilizzo dei set di risorse in Firewall Manager
- Visualizzazione delle informazioni sulla conformità per una AWS Firewall Manager politica
- AWS Firewall Manager scoperte
- Sicurezza in AWS Firewall Manager
- AWS Firewall Manager quote

AWS Firewall Manager prezzi

I costi sostenuti da AWS Firewall Manager si riferiscono ai servizi sottostanti, ad esempio AWS WAF e AWS Config. Per ulteriori informazioni, consultare Prezzi di AWS Firewall Manager.

AWS Firewall Manager prerequisiti

In questo argomento viene illustrato come prepararsi all'amministrazione AWS Firewall Manager. È possibile utilizzare un account amministratore di Firewall Manager per gestire tutte le politiche di sicurezza di Firewall Manager per l'organizzazione in AWS Organizations. Salvo dove indicato, esegui i passaggi preliminari utilizzando l'account che utilizzerai come amministratore di Firewall Manager.

Prima di utilizzare Firewall Manager per la prima volta, eseguire i seguenti passaggi in sequenza.

Argomenti

- Fase 1: Partecipa e configura AWS Organizations
- Passaggio 2: creare un account amministratore AWS Firewall Manager predefinito
- Fase 3: Attivazione AWS Config
- Passaggio 4: Per le politiche di terze parti, iscriviti al AWS Marketplace e configura le impostazioni di terze parti
- Passaggio 5: per le politiche Network Firewall e DNS Firewall, abilitare la condivisione delle risorse
- Passaggio 6: Da utilizzare AWS Firewall Manager nelle regioni disattivate per impostazione predefinita

Fase 1: Partecipa e configura AWS Organizations

Per utilizzare Firewall Manager, l'account deve essere membro dell'organizzazione del AWS Organizations servizio in cui si desidera utilizzare le politiche di Firewall Manager.

> **Note**
>
> Per informazioni su Organizations, consulta la AWS Organizations User Guide.

Per stabilire l' AWS Organizations appartenenza e la configurazione richieste

1. Scegli un account da utilizzare come amministratore di Firewall Manager per l'organizzazione in Organizations.
2. Se l'account che hai scelto non è già membro dell'organizzazione, fallo iscrivere. Segui le indicazioni riportate in Invitare un uomo Account AWS a entrare a far parte della tua organizzazione.
3. AWS Organizations dispone di due set di funzionalità: funzionalità di fatturazione consolidata e tutte le funzionalità. Per utilizzare Firewall Manager, l'organizzazione deve essere abilitata per tutte le funzionalità. Se l'organizzazione è configurata solo per la fatturazione consolidata, segui le indicazioni riportate nella sezione Abilitazione di tutte le funzionalità dell'organizzazione.

Passaggio 2: creare un account amministratore AWS Firewall Manager predefinito

Questa procedura utilizza l'account e l'organizzazione scelti e configurati nel passaggio precedente.

Solo l'account di gestione dell'organizzazione può creare account amministratore predefiniti di Firewall Manager. Il primo account amministratore creato è l'account amministratore predefinito. L'account amministratore predefinito può gestire firewall di terze parti e dispone di un ambito amministrativo completo. Quando si imposta l'account amministratore predefinito, Firewall Manager lo imposta automaticamente come amministratore AWS Organizations delegato per Firewall Manager. Ciò consente a Firewall Manager di accedere alle informazioni sulle unità organizzative (OU) dell'organizzazione. È possibile utilizzare le unità organizzative per specificare l'ambito delle politiche di Firewall Manager. Per ulteriori informazioni sull'impostazione dell'ambito delle politiche, consulta le linee guida per i singoli tipi di policy riportate di seguitoCreazione di una AWS Firewall Manager politica. Per ulteriori informazioni su Organizations e management account, vedere Managing the AWS Accounts in Your Organization.

Impostazioni richieste per l'account di gestione dell'organizzazione

L'account di gestione dell'organizzazione deve avere le seguenti impostazioni per effettuare l'onboarding dell'organizzazione in Firewall Manager e creare un amministratore predefinito:

- Deve essere un membro dell'organizzazione a AWS Organizations cui desideri applicare le policy di Firewall Manager.

Per impostare l'account amministratore predefinito

1. Accedere a Firewall Manager AWS Management Console utilizzando un account di AWS Organizations gestione esistente.
2. Apri la console di Firewall Manager all'indirizzo https://console.aws.amazon.com/wafv2/fmsv2.
3. Nel pannello di navigazione scegli Impostazioni.
4. Digita l' AWS ID dell'account che hai scelto di utilizzare come amministratore di Firewall Manager.

   > **Note**
   >
   > L'amministratore predefinito ha un ambito amministrativo completo. L'ambito amministrativo completo significa che questo account può applicare politiche a tutti gli account e le unità organizzative (OU) all'interno dell'organizzazione, intraprendere azioni in tutte le regioni e gestire tutti i tipi di policy di Firewall Manager.

5. Scegli Crea account amministratore per creare l'account.

Per ulteriori informazioni sulla gestione dell'account amministratore di Firewall Manager, vedereCollaborazione con AWS Firewall Manager gli amministratori.

Fase 3: Attivazione AWS Config

Per utilizzare Firewall Manager, è necessario abilitare AWS Config.

> **Note**
>
> Le AWS Config impostazioni sono soggette a costi aggiuntivi, in base ai AWS Config prezzi. Per ulteriori informazioni, consulta la sezione Guida introduttiva. AWS Config

> **Note**
>
> Affinché Firewall Manager possa monitorare la conformità delle policy, AWS Config deve registrare continuamente le modifiche alla configurazione per le risorse protette. Nella AWS Config configurazione, la frequenza di registrazione deve essere impostata su Continuo, che è l'impostazione predefinita.

AWS Config Per abilitare Firewall Manager

1. Abilita AWS Config per ogni account AWS Organizations membro, incluso l'account amministratore di Firewall Manager. Per ulteriori informazioni, vedere Guida introduttiva a AWS Config.
2. Abilita AWS Config per ognuno Regione AWS che contiene le risorse che desideri proteggere. Puoi AWS Config abilitarlo manualmente oppure puoi utilizzare il AWS CloudFormation modello «Enable AWS Config» in AWS CloudFormation StackSets Sample Templates.

   Se non desideri abilitare tutte AWS Config le risorse, devi abilitare quanto segue in base al tipo di policy di Firewall Manager che utilizzi:

   - Politica WAF: abilita Config per i CloudFront tipi di risorse Distribution, Application Load Balancer ElasticLoadBalancing(scegli V2 dall'elenco), API Gateway, WAF WebACL, WAF Regional WebACL e WAFV2 WebACL. Per abilitare la protezione di una distribuzione, devi trovarti AWS Config nella regione Stati Uniti orientali (Virginia settentrionale CloudFront). Le altre regioni non dispongono CloudFront di alcuna opzione.
   - Politica Shield: abilita Config per i tipi di risorse Shield Protection, ShieldRegional Protection, Application Load Balancer, EC2 EIP, WAF WebACL, WAF Regional WebACL e WAFV2 WebACL.
   - Politica del gruppo di sicurezza: abilita Config per i tipi di risorse EC2 SecurityGroup, EC2 Instance ed EC2. NetworkInterface
   - Politica Network Firewall: abilita Config per i tipi di risorse, EC2 VPC NetworkFirewall FirewallPolicy NetworkFirewallRuleGroup, EC2, InternetGateway EC2 e EC2 Subnet. RouteTable
   - Politica DNS Firewall: abilita Config per il tipo di risorsa EC2 VPC.

- Policy firewall di terze parti: abilita Config per i tipi di risorse Amazon EC2 VPC, Amazon EC2, Amazon EC2, Amazon InternetGateway EC2 Subnet e Amazon RouteTable EC2 VPCEndpoint.

> **Note**
>
> Se configuri il AWS Config registratore per utilizzare un ruolo IAM personalizzato, devi assicurarti che la policy IAM disponga delle autorizzazioni appropriate per registrare i tipi di risorse richiesti dalla policy Firewall Manager. Senza le autorizzazioni appropriate, le risorse richieste potrebbero non essere registrate, il che impedisce a Firewall Manager di proteggere adeguatamente le risorse. Firewall Manager non ha visibilità su queste configurazioni errate delle autorizzazioni. Per informazioni sull'utilizzo di IAM con AWS Config, consulta IAM for. AWS Config

Passaggio 4: Per le politiche di terze parti, iscriviti al AWS Marketplace e configura le impostazioni di terze parti

Completa i seguenti prerequisiti per iniziare a utilizzare le politiche firewall di terze parti di Firewall Manager.

Prerequisiti della politica Fortigate Cloud Native Firewall (CNF) as a Service

Per utilizzare Fortigate CNF per Firewall Manager

1. Abbonati al servizio Fortigate Cloud Native Firewall (CNF) as a Service nel Marketplace. AWS
2. Innanzitutto, registra un inquilino sul portale dei prodotti Fortigate CNF. Quindi aggiungi il tuo account amministratore di Firewall Manager sotto il tuo tenant sul portale dei prodotti Fortigate CNF. Per ulteriori informazioni, consulta la documentazione di Fortigate CNF.

Per informazioni sull'utilizzo delle politiche CNF di Fortigate, vedere. Politiche di Fortigate Cloud Native Firewall (CNF) as a Service

Prerequisiti della policy Palo Alto Networks Cloud Next Generation Firewall

Per utilizzare Palo Alto Networks Cloud NGFW per Firewall Manager

1. Abbonati al servizio Palo Alto Networks Cloud Next Generation Firewall Pay-As-You-Go nel Marketplace. AWS
2. Completa i passaggi di implementazione di Palo Alto Networks Cloud NGFW elencati nella sezione Deploy Palo Alto Networks Cloud NGFW per AWS con l'argomento nella guida Palo Alto Networks Cloud Next Generation Firewall per l' AWS Firewall Managerimplementazione. AWS

Per informazioni sull'utilizzo delle politiche NGFW di Palo Alto Networks Cloud, vedere. Politiche NGFW di Palo Alto Networks Cloud

Passaggio 5: per le politiche Network Firewall e DNS Firewall, abilitare la condivisione delle risorse

Per gestire le politiche Firewall Manager Network Firewall e DNS Firewall, è necessario abilitare la condivisione con AWS Organizations in AWS Resource Access Manager. Ciò consente a Firewall Manager di implementare protezioni su tutti gli account quando si creano questi tipi di policy.

Per abilitare la condivisione con in AWS OrganizationsAWS Resource Access Manager

- Segui le indicazioni riportate nella sezione Abilita la condivisione con AWS Organizations nella Guida AWS Resource Access Manager per l'utente.

Se riscontri problemi con la condivisione delle risorse, consulta la guida all'indirizzoCondivisione delle risorse per le politiche Network Firewall e DNS Firewall.

Passaggio 6: Da utilizzare AWS Firewall Manager nelle regioni disattivate per impostazione predefinita

Per utilizzare Firewall Manager in un'area che è disabilitata per impostazione predefinita, è necessario abilitare la regione sia per l'account di gestione dell' AWS organizzazione che per l'account amministratore predefinito di Firewall Manager. Per informazioni sulle regioni che sono disabilitate per impostazione predefinita e su come attivarle, vedere Gestione Regioni AWS nella AWS Guida generale.

Per abilitare una regione disattivata

- Sia per l'account di gestione Organizations che per l'account amministratore predefinito di Firewall Manager, segui le indicazioni riportate in Enabling a Region nella Guida AWS generale.

Dopo aver seguito questi passaggi, puoi configurare Firewall Manager per iniziare a proteggere le tue risorse. Per ulteriori informazioni, consulta Guida introduttiva alle AWS Firewall ManagerAWS WAF politiche.

Collaborazione con AWS Firewall Manager gli amministratori

Con AWS Firewall Manager puoi avere uno o più amministratori in grado di gestire le risorse firewall della tua organizzazione. Se si desidera utilizzare più amministratori di Firewall Manager nella propria organizzazione, è possibile applicare condizioni di ambito amministrativo a ciascun amministratore per definire le risorse che può gestire. Ciò offre la flessibilità necessaria per avere diversi ruoli di amministratore all'interno dell'organizzazione e aiuta a mantenere il principio dell'accesso con privilegi minimi. Ad esempio, è possibile fare in modo che un amministratore gestisca un set di unità organizzative (OU) per l'organizzazione, delegando a un altro amministratore la gestione solo di tipi di policy di Firewall Manager specifici. Per ulteriori informazioni su Organizations e management account, vedere Managing the AWS Accounts in Your Organization.

Per il numero massimo di amministratori che puoi avere per organizzazione, vedi AWS Firewall Manager quote

Guida introduttiva all'utilizzo degli amministratori di Firewall Manager

Prima di iniziare a utilizzare gli amministratori di Firewall Manager, è necessario completare i prerequisiti elencati in. AWS Firewall Manager prerequisiti Nei prerequisiti, effettuerai l'onboarding di un' AWS Organizations organizzazione in Firewall Manager e creerai un account amministratore predefinito per Firewall Manager. Un account amministratore predefinito è in grado di gestire firewall di terze parti e dispone di un ambito amministrativo completo.

Ambito amministrativo

L'ambito amministrativo definisce le risorse che l'amministratore di Firewall Manager può gestire. Dopo che un account di AWS Organizations gestione ha integrato un'organizzazione in Firewall Manager, l'account di gestione può creare amministratori di Firewall Manager aggiuntivi con diversi ambiti amministrativi. Un account AWS Organizations di gestione può concedere all'amministratore un ambito amministrativo completo o limitato. L'ambito completo offre all'amministratore l'accesso

completo a tutti i tipi di risorse precedenti. L'ambito limitato si riferisce alla concessione di autorizzazioni amministrative solo a un sottoinsieme delle risorse precedenti. Si consiglia di concedere agli amministratori solo le autorizzazioni necessarie per svolgere i compiti previsti dal loro ruolo. È possibile applicare qualsiasi combinazione di queste condizioni di ambito amministrativo a un amministratore:

- Account o unità organizzative dell'organizzazione a cui l'amministratore può applicare i criteri.
- Regioni in cui l'amministratore può eseguire azioni.
- Tipi di policy di Firewall Manager che l'amministratore può gestire.

Ruoli di amministratore

Esistono due tipi di ruoli di amministratore in Firewall Manager: un amministratore predefinito e gli amministratori di Firewall Manager.

- Amministratore predefinito: l'account di gestione dell'organizzazione crea un account amministratore predefinito di Firewall Manager quando esegue l'onboarding dell'organizzazione in Firewall Manager durante il completamento delAWS Firewall Manager prerequisiti. L'amministratore predefinito può gestire i firewall di terze parti e dispone di un ambito amministrativo completo, ma per il resto ha lo stesso livello di pari livello degli altri amministratori, se si sceglie di avere più amministratori.
- Amministratori di Firewall Manager: un amministratore di Firewall Manager può gestire le risorse che l'account di AWS Organizations gestione gli assegna nella configurazione dell'ambito amministrativo. Per il numero massimo di amministratori che puoi avere per organizzazione, vedi. AWS Firewall Manager quote Al momento della creazione di un account amministratore di Firewall Manager, il servizio verifica con AWS Organizations se l'account è già un amministratore delegato per Firewall Manager all'interno dell'organizzazione. In caso contrario, Firewall Manager chiama Organizations per impostare l'account come amministratore delegato per Firewall Manager. Per informazioni sugli amministratori delegati di Organizations, vedere la AWS Organizations terminologia e i concetti nella Guida per l'AWS Organizations utente.

Amministratori esistenti

Se sei già cliente di Firewall Manager e hai già impostato un amministratore, questo amministratore esistente sarà l'amministratore predefinito di Firewall Manager. Non dovrebbero esserci impatti sul flusso esistente. Se desideri aggiungere altri amministratori, puoi farlo seguendo le procedure descritte in questo capitolo.

Creazione, aggiornamento e revoca degli account amministratore di Firewall Manager

Le procedure riportate nei seguenti argomenti spiegano come creare, aggiornare e revocare gli account amministratore di Firewall Manager. Solo l'account di gestione di un'organizzazione può creare e aggiornare gli account amministratore di Firewall Manager. Solo un singolo amministratore di Firewall Manager può revocare il proprio account amministratore.

Creazione di un account amministratore di Firewall Manager

La procedura seguente descrive come creare un account di amministratore di Firewall Manager utilizzando la console Firewall Manager.

Per creare un account amministratore di Firewall Manager

1. Accedere a Firewall Manager AWS Management Console utilizzando un account di AWS Organizations gestione esistente.
2. Apri la console di Firewall Manager all'indirizzo https://console.aws.amazon.com/wafv2/fmsv2.
3. Nel pannello di navigazione scegli Impostazioni.
4. Scegli Crea account amministratore.
5. Nel riquadro Dettagli, per l'ID dell'AWS account, digita l' AWS ID di un account membro che desideri aggiungere come amministratore di Firewall Manager.
6. Per Ambito amministrativo, scegli una delle seguenti opzioni:

   - Completo: consente all'amministratore di applicare le policy a tutti gli account e le unità organizzative (OU) all'interno dell'organizzazione, intraprendere azioni in tutte le regioni e applicare tutti i tipi di policy di Firewall Manager, ad eccezione dei firewall di terze parti. Solo l'amministratore predefinito può creare e gestire firewall di terze parti. Fai attenzione se concedi questo livello di autorizzazioni all'amministratore. Nello spirito del privilegio minimo, consigliamo di concedere all'amministratore solo le autorizzazioni necessarie per svolgere i compiti previsti dal suo ruolo.
   - Limitato: se applichi un ambito limitato, in Configura l'ambito amministrativo configura gli account e le unità organizzative, le regioni e i tipi di policy che l'account può gestire.

     Per Account e unità organizzative, scegli le opzioni seguenti:

     - Se desideri applicare le politiche a tutti gli account o le unità organizzative della tua organizzazione, scegli Includi tutti gli account nella mia AWS organizzazione.

- Se desideri applicare i criteri solo a conti specifici o account che si trovano in unità AWS Organizations organizzative (OU) specifiche, scegli Includi solo gli account e le unità organizzative specificati, quindi aggiungi gli account e le unità organizzative che desideri includere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.
- Se desideri applicare i criteri a tutti i conti o le unità AWS Organizations organizzative (OU) tranne uno specifico, scegli Escludi gli account e le unità organizzative specificati e includi tutti gli altri, quindi aggiungi gli account e le unità organizzative che desideri escludere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

Per le regioni, scegli le opzioni seguenti:

- Se desideri consentire all'amministratore di eseguire azioni in tutte le regioni disponibili, scegli Includi tutte le regioni.
- Se desideri che l'amministratore esegua azioni solo in regioni specifiche, scegli Includi solo le regioni specificate, quindi specifica le regioni che desideri includere.

> **Note**
>
> Per includere una regione disabilitata per impostazione predefinita, è necessario abilitare la regione sia per l'account di gestione AWS Organizations dell'organizzazione che per l'account di amministrazione predefinito. Per informazioni sull'attivazione delle regioni per un account, consulta Abilitare una regione in Riferimenti generali di Amazon Web Services.

Per i tipi di policy, scegli le opzioni come segue:.

- Se desideri consentire all'amministratore di gestire tutti i tipi di policy, scegli Includi tutti i tipi di policy.
- Se desideri che l'amministratore gestisca solo tipi di policy specifici, scegli Includi solo i tipi di policy specificati, quindi specifica i tipi di policy che desideri includere.

7. Scegli Crea account amministratore per creare l'account amministratore. Al momento della creazione, Firewall Manager effettua una chiamata AWS Organizations per verificare se l'amministratore è già un amministratore delegato dell'organizzazione. In caso contrario,

Firewall Manager designerà l'account come amministratore delegato. Per informazioni sugli amministratori delegati in Organizations, consulta la AWS Organizations terminologia e i concetti nella Guida per l'AWS Organizations utente.

Se si applica un ambito amministrativo limitato, Firewall Manager valuta automaticamente tutte le nuove risorse in base alle impostazioni dell'utente. Ad esempio, se includi solo account specifici, Firewall Manager non applica la politica a nessun nuovo account. Come altro esempio, se si include un'unità organizzativa, quando si aggiunge un account all'unità organizzativa o a una delle relative unità organizzative secondarie, Firewall Manager include automaticamente l'account nell'ambito amministrativo.

Aggiornamento di un account amministratore di Firewall Manager

La procedura seguente descrive come aggiornare un account amministratore di Firewall Manager utilizzando la console Firewall Manager.

> **Note**
>
> Per aggiornare l'ambito di un amministratore in modo da includere una regione disabilitata per impostazione predefinita, è necessario abilitare la regione sia per l'account di gestione AWS Organizations dell'organizzazione che per l'account di amministrazione predefinito. Per informazioni sull'attivazione delle regioni per un account, consulta Abilitare una regione in Riferimenti generali di Amazon Web Services.

Per aggiornare un account amministratore (console)

1. Accedere a Firewall Manager AWS Management Console utilizzando un account di AWS Organizations gestione esistente.
2. Apri la console di Firewall Manager all'indirizzo https://console.aws.amazon.com/wafv2/fmsv2.
3. Nel pannello di navigazione scegli Impostazioni.
4. nella tabella degli amministratori di Firewall Manager, scegli l'account che desideri aggiornare.
5. Seleziona Modifica per modificare i dettagli dell'account dell'amministratore. Non puoi modificare l'ID dell'account.
6. Scegliere Salva per salvare le modifiche.

Revoca di un account amministratore

La procedura seguente descrive come revocare un account amministratore di Firewall Manager. Se sei l'amministratore predefinito, prima di poter revocare il tuo account, tutti gli account amministratore di Firewall Manager all'interno dell'organizzazione devono prima revocare i propri account. Per revocare un account amministratore, segui la procedura seguente

Per revocare un account amministratore (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.
2. Nel pannello di navigazione scegli Impostazioni.
3. Nel riquadro Account amministratore, seleziona Revoca account amministratore per revocare l'account.

> **Important**
>
> Quando si revocano i privilegi di amministratore a un account amministratore, tutte le politiche di Firewall Manager create da tale account vengono eliminate.

Modifica dell'account amministratore predefinito

È possibile designare un solo account in un'organizzazione come account amministratore predefinito di Firewall Manager. L'account amministratore predefinito segue il principio «first in, last out». Per designare un account amministratore predefinito diverso, ogni singolo account amministratore deve prima revocare il proprio account. Quindi, l'amministratore predefinito esistente può revocare il proprio account, eliminando così l'organizzazione da Firewall Manager. Quando un amministratore revoca il proprio account, tutte le politiche di Firewall Manager create da quell'account vengono eliminate. Per designare un nuovo account amministratore predefinito, è quindi necessario accedere a Firewall Manager con l'account di AWS Organizations gestione per designare un nuovo account amministratore. Per modificare l'account amministratore predefinito per un'organizzazione, eseguire la procedura seguente.

Per modificare l'account amministratore predefinito

1. Accedere a Firewall Manager AWS Management Console utilizzando un account di AWS Organizations gestione esistente.
2. Apri la console di Firewall Manager all'indirizzo https://console.aws.amazon.com/wafv2/fmsv2.
3. Nel pannello di navigazione scegli Impostazioni.
4. Digita l'ID dell'account che hai scelto di utilizzare come amministratore di Firewall Manager.

> **Note**
>
> A questo account viene concessa l'autorizzazione a creare e gestire le politiche di Firewall Manager per tutti gli account all'interno dell'organizzazione.

5. Scegli Crea account amministratore.
6. Digita l' AWS ID dell'account che hai scelto di utilizzare come amministratore di Firewall Manager.

> **Note**
>
> A questo account viene assegnato l'ambito amministrativo completo. L'ambito amministrativo completo significa che questo account può applicare politiche a tutti gli account e le unità organizzative (OU) all'interno dell'organizzazione, intraprendere azioni in tutte le regioni e gestire tutti i tipi di policy di Firewall Manager.

7. Scegli Crea account amministratore per creare l'account amministratore predefinito.

Escludere le modifiche a un account amministratore

Alcune modifiche a un account amministratore possono impedirgli di rimanere un account amministratore.

Questa sezione descrive le modifiche che possono squalificare un account amministratore AWS e come Firewall Manager gestiscono queste modifiche.

Account rimosso dall'organizzazione in AWS Organizations

Se l'account AWS Firewall Manager amministratore viene rimosso dall'organizzazione nel AWS Organizations, non può più amministrare le politiche per l'organizzazione. Firewall Manager esegue una delle seguenti azioni:

- Account senza policy: se l'account amministratore di Firewall Manager non ha policy di Firewall Manager, Firewall Manager revoca l'account amministratore.
- Account con policy Firewall Manager: se l'account amministratore di Firewall Manager dispone di policy di Firewall Manager, Firewall Manager invia un'e-mail per informarvi della situazione e indicarvi le opzioni possibili, con l'aiuto del vostro rappresentante AWS commerciale.

Account chiuso

Se chiudi l'account che stai utilizzando per l' AWS Firewall Manager amministratore AWS e Firewall Manager gestisci la chiusura come segue:

- AWS revoca l'accesso di amministratore dell'account da Firewall Manager e Firewall Manager disattiva tutte le politiche gestite dall'account amministratore. Le protezioni fornite da tali policy vengono interrotte in tutta l'organizzazione.
- AWS conserva i dati delle policy di Firewall Manager per l'account per 90 giorni dalla data effettiva di chiusura dell'account amministratore. Durante questo periodo di 90 giorni, è possibile riaprire l'account chiuso.
  - Se riapri l'account chiuso durante il periodo di 90 giorni, AWS riassegna l'account come amministratore di Firewall Manager e recupera i dati delle policy di Firewall Manager per l'account.
  - Altrimenti, al termine del periodo di 90 giorni, elimina AWS definitivamente tutti i dati delle policy di Firewall Manager per l'account.

Guida introduttiva alle AWS Firewall Manager politiche

È possibile utilizzare AWS Firewall Manager per abilitare diversi tipi di politiche di sicurezza. I passaggi per la configurazione sono leggermente diversi per ciascuno.

Argomenti

- Guida introduttiva alle AWS Firewall ManagerAWS WAF politiche

- Guida introduttiva alle AWS Firewall ManagerAWS Shield Advanced politiche
- Guida introduttiva alle policy dei gruppi di sicurezza di AWS Firewall Manager Amazon VPC
- Guida introduttiva alle AWS Firewall ManagerAWS Network Firewall politiche
- Guida introduttiva alle AWS Firewall Manager politiche del firewall DNS
- Guida introduttiva alle policy di AWS Firewall Manager Palo Alto Networks Cloud Next Generation Firewall
- Guida introduttiva alle politiche di AWS Firewall Manager Fortigate CNF

Guida introduttiva alle AWS Firewall ManagerAWS WAF politiche

AWS Firewall Manager Per abilitare AWS WAF le regole in tutta l'organizzazione, esegui i seguenti passaggi in sequenza.

Argomenti

- Fase 1: completamento dei prerequisiti
- Fase 2: Creare e applicare una AWS WAF policy
- Fase 3: elimina

Fase 1: completamento dei prerequisiti

Vi sono diversi passaggi obbligatori per preparare l'account AWS Firewall Manager. Tali fasi sono descritte nell'articolo AWS Firewall Manager prerequisiti. Completare tutti i prerequisiti prima di passare a Fase 2: Creare e applicare una AWS WAF policy.

Fase 2: Creare e applicare una AWS WAF policy

Una AWS WAF politica di Firewall Manager contiene i gruppi di regole che desideri applicare alle tue risorse. Firewall Manager crea un ACL web di Firewall Manager in ogni account a cui si applica la policy. I singoli responsabili dell'account possono aggiungere regole e gruppi di regole alla ACL Web risultante, oltre ai gruppi di regole definiti qui. Per informazioni sulle AWS WAF politiche di Firewall Manager, vedereAWS WAF politiche.

Per creare una AWS WAF policy di Firewall Manager (console)

Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2.

Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

1. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
2. Scegli Crea policy.
3. Per Policy type (Tipo di policy), scegliere AWS WAF.
4. Per Regione, scegli un Regione AWS. Per proteggere le CloudFront distribuzioni Amazon, scegli Global.

   Per proteggere le risorse in più regioni (diverse dalle CloudFront distribuzioni), è necessario creare policy Firewall Manager separate per ogni regione.
5. Seleziona Successivo.
6. Per Nome della politica, inserire un nome descrittivo. Firewall Manager include il nome della policy nei nomi degli ACL Web che gestisce. I nomi degli ACL Web sono `FMManagedWebACLV2-` seguiti dal nome della policy immesso qui e dal timestamp di creazione degli ACL Web-, in millisecondi UTC. Ad esempio, `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`.

   > **Important**
   >
   > I nomi ACL Web non possono cambiare dopo la creazione. Se aggiorni il nome della policy, Firewall Manager non aggiornerà il nome ACL web associato. Per fare in modo che Firewall Manager crei un ACL Web con un nome diverso, è necessario creare una nuova policy.
7. In Policy rules, per First rule groups, scegli Aggiungi gruppi di regole. Espandi i gruppi di regole AWS gestiti. Per il set di regole di base, attivare Add to web ACL (Aggiungi alla ACL Web). Per gli input AWS noti non validi, attiva Aggiungi all'ACL web. Scegliere Add rules (Aggiungi regole).

   Per Last rule groups (Ultimi gruppi di regole), scegliere Add rule groups (Aggiungi gruppi di regole). Espandi i gruppi di regole AWS gestiti e, per l'elenco di reputazione degli IP di Amazon, attiva Aggiungi all'ACL web. Scegliere Add rules (Aggiungi regole).

   In First rule groups, seleziona Set di regole di base e scegli Sposta giù. AWS WAF valuta le richieste Web in base al AWS noto gruppo di regole di input non validi prima di eseguire la valutazione rispetto al set di regole Core.

Puoi anche creare i tuoi gruppi di AWS WAF regole, se lo desideri, utilizzando la console. AWS WAF Tutti i gruppi di regole creati vengono visualizzati in Your rule groups (Gruppi di regole personali) nella pagina Describe policy : Add rule groups (Descrizione della policy: aggiungi gruppi di regole).

Il primo e l'ultimo gruppo di AWS WAF regole gestiti tramite Firewall Manager hanno nomi che iniziano con `PREFMManaged-` o`POSTFMManaged-`, rispettivamente, seguiti dal nome della policy di Firewall Manager e dal timestamp di creazione del gruppo di regole, in millisecondi UTC. Ad esempio, `PREFMManaged-MyWAFPolicyName-1621880555123`.

8. Lasciare l'azione predefinita per l'ACL Web in Allow (Consenti).
9. Lasciare l'azione Policy predefinita per non correggere automaticamente le risorse non conformi. È possibile modificare l'opzione in un secondo momento.
10. Seleziona Successivo.
11. Per l' ambito Policy, si forniscono le impostazioni per gli account, i tipi di risorse e i tag che identificano le risorse a cui si desidera applicare la policy. Per questo tutorial, esci dalle impostazioni Account AWSe Risorse e scegli uno o più tipi di risorse.
12. Seleziona Successivo.
13. Per i tag Policy, è possibile aggiungere qualsiasi tag identificativo desiderato per la AWS WAF policy Firewall Manager. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor . Per questo tutorial, è possibile lasciare i tag vuoti.
14. Seleziona Successivo.
15. Rivedere la nuova policy. È possibile apportare modifiche scegliendo Edit (Modifica) nell'area che si desidera modificare. In questo modo si torna al passaggio corrispondente della creazione guidata. Al termine, scegliere Create policy (Crea policy).

Fase 3: elimina

Per evitare addebiti imprevisti, eliminare tutte le policy e le risorse non necessarie.

Per eliminare una policy (console)

1. Nella pagina delle AWS Firewall Manager politiche, scegli il pulsante di opzione accanto al nome della politica, quindi scegli Elimina.
2. Nella casella di conferma Delete (Elimina) selezionare Delete all policy resources (Elimina tutte le risorse di policy), quindi scegliere di nuovo Delete (Elimina).

AWS WAF rimuove la policy e tutte le risorse associate, come gli ACL web, che ha creato nel tuo account. La propagazione delle modifiche in tutti gli account potrebbe richiedere alcuni minuti.

Guida introduttiva alle AWS Firewall ManagerAWS Shield Advanced politiche

Puoi utilizzarlo AWS Firewall Manager per abilitare AWS Shield Advanced le protezioni in tutta l'organizzazione.

> **Important**
>
> Firewall Manager non supporta Amazon Route 53 o AWS Global Accelerator. Se devi proteggere queste risorse con Shield Advanced, non puoi utilizzare una policy Firewall Manager. Seguire invece le istruzioni in Aggiungere AWS Shield Advanced protezione alle risorse AWS.

Per utilizzare Firewall Manager per abilitare la protezione Shield Advanced, eseguire i seguenti passaggi in sequenza.

Argomenti

Fase 1: completamento dei prerequisiti

Vi sono diversi passaggi obbligatori per preparare l'account AWS Firewall Manager. Tali fasi sono descritte nell'articolo AWS Firewall Manager prerequisiti. Completare tutti i prerequisiti prima di passare a Fase 2: Creare e applicare una policy Shield Advanced.

Fase 2: Creare e applicare una policy Shield Advanced

Dopo aver completato i prerequisiti, crei una politica AWS Firewall Manager Shield Advanced. Una policy Firewall Manager Shield Advanced contiene gli account e le risorse che desideri proteggere con Shield Advanced.

> **Important**
>
> Firewall Manager non supporta Amazon Route 53 o AWS Global Accelerator. Se devi proteggere queste risorse con Shield Advanced, non puoi utilizzare una policy Firewall Manager. Seguire invece le istruzioni in Aggiungere AWS Shield Advanced protezione alle risorse AWS.

Per creare una policy Firewall Manager Shield Advanced (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Scegli Crea policy.
4. Per Tipo di policy, scegli Shield Advanced.

   Per creare una policy Shield Advanced, l'account amministratore di Firewall Manager deve essere abbonato a Shield Advanced. Se non si è iscritti, viene richiesto di farlo. Per informazioni sul costo dell'abbonamento, consulta AWS Shield Advanced Prezzi.

   > **Note**
   >
   > Non è necessario sottoscrivere manualmente ogni account membro a Shield Advanced. Firewall Manager esegue questa operazione automaticamente al momento della

creazione della policy. Ogni account deve rimanere abbonato a Firewall Manager e Shield Advanced per continuare a proteggere le risorse dell'account.

5. Per Regione, scegli un Regione AWS. Per proteggere CloudFront le risorse di Amazon, scegli Global.

   Per proteggere le risorse in più regioni (diverse dalle CloudFront risorse), è necessario creare policy Firewall Manager separate per ogni regione.
6. Seleziona Successivo.
7. Per Nome, inserisci un nome descrittivo.
8. (Solo regione globale) Per le politiche dell'area globale, puoi scegliere se gestire la mitigazione degli attacchi DDoS a livello di applicazione automatica Shield Advanced. Per questo tutorial, lascia questa scelta all'impostazione predefinita di Ignora.
9. Per l'azione politica, scegli l'opzione che non corregge automaticamente.
10. Seleziona Successivo.
11. Account AWS questa politica si applica e consente di restringere l'ambito della politica specificando gli account da includere o escludere. Per questa esercitazione, scegliere Includi tutti gli account nell'organizzazione.
12. Scegliere i tipi di risorse da proteggere.

    Firewall Manager non supporta Amazon Route 53 o AWS Global Accelerator. Se devi proteggere queste risorse con Shield Advanced, non puoi utilizzare una policy Firewall Manager. Segui invece la guida Shield Advanced all'indirizzoAggiungere AWS Shield Advanced protezione alle risorse AWS.
13. Se desideri proteggere solo risorse con tag specifici o, in alternativa, escludere risorse con tag specifici, seleziona Usa tag per includere/escludere risorse, inserisci i tag separati da virgole, quindi scegli Includi o Escludi. È possibile scegliere una sola opzione.

    Se inserisci più di un tag e se una risorsa ha uno di questi tag, viene considerata una corrispondenza.

    Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .
14. Seleziona Successivo.
15. Per i tag Policy, aggiungi tutti i tag identificativi che desideri per la policy di Firewall Manager. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .
16. Seleziona Successivo.

17. Rivedere la nuova policy. Per apportare modifiche, scegliere Previous (Precedente). Al termine, scegliere Create policy (Crea policy).

Continua su Fase 3: (Facoltativo) autorizzare lo Shield Response Team (SRT).

Fase 3: (Facoltativo) autorizzare lo Shield Response Team (SRT)

Uno dei vantaggi di AWS Shield Advanced è il supporto dello Shield Response Team (SRT). In caso di potenziale attacco DDoS, puoi contattare il AWS Support Centro. Se necessario, il Support Center inoltra il problema all'SRT. L'SRT ti aiuta ad analizzare le attività sospette e ti aiuta a mitigare il problema. Questa mitigazione spesso comporta la creazione o l'aggiornamento di AWS WAF regole e ACL Web nel tuo account. L'SRT può ispezionare la AWS WAF configurazione e creare o aggiornare AWS WAF regole e ACL Web per conto vostro, ma il team ha bisogno della vostra autorizzazione per farlo. Come parte della configurazione AWS Shield Advanced, si consiglia di fornire in modo proattivo all'SRT l'autorizzazione necessaria. Concedere in anticipo l'autorizzazione consente di evitare ritardi relativi alla mitigazione in caso di attacco imminente.

Autorizzi e contatti l'SRT a livello di account. Cioè, il proprietario dell'account, non l'amministratore di Firewall Manager, deve eseguire i seguenti passaggi per autorizzare l'SRT a mitigare i potenziali attacchi. L'amministratore di Firewall Manager può autorizzare l'SRT solo per gli account di sua proprietà. Allo stesso modo, solo il proprietario dell'account può contattare l'SRT per ricevere assistenza.

> **Note**
>
> Per utilizzare i servizi dell'SRT, è necessario essere abbonati al piano Business Support o al piano Enterprise Support.

Per autorizzare l'SRT a mitigare i potenziali attacchi per tuo conto, segui le istruzioni riportate in. Supporto dello Shield Response Team (SRT) Puoi modificare l'accesso e le autorizzazioni SRT in qualsiasi momento seguendo la stessa procedura.

Continua su Fase 4: Configurazione delle notifiche e degli allarmi Amazon SNS CloudWatch .

Fase 4: Configurazione delle notifiche e degli allarmi Amazon SNS CloudWatch

Puoi continuare da questo passaggio senza configurare le notifiche CloudWatch o gli allarmi di Amazon SNS. Tuttavia, la configurazione di questi allarmi e notifiche aumenta in modo significativo la visibilità su possibili eventi DDoS.

Puoi monitorare le tue risorse protette per potenziali attività DDoS utilizzando Amazon SNS. Per ricevere notifiche di possibili attacchi, crea un argomento Amazon SNS per ogni regione.

Per creare un argomento Amazon SNS in Firewall Manager (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel pannello di navigazione, sotto AWS FMS, scegli Impostazioni.
3. Scegli Create new topic (Crea nuovo argomento).
4. Inserisci un nome dell'argomento.
5. Inserisci un indirizzo e-mail a cui verranno inviati i messaggi Amazon SNS, quindi scegli Aggiungi indirizzo e-mail.
6. Selezionare Update SNS configuration (Aggiorna configurazione SNS).

Configurazione degli CloudWatch allarmi Amazon

Shield Advanced consente il rilevamento, la mitigazione e le metriche dei principali contributori in modo CloudWatch che sia possibile monitorare. Per ulteriori informazioni, consulta. AWS Shield Advanced metriche CloudWatch comporta costi aggiuntivi. Per CloudWatch i prezzi, consulta la pagina CloudWatch dei prezzi di Amazon.

Per creare un CloudWatch allarme, segui le istruzioni in Uso di Amazon CloudWatch Alarms. Per impostazione predefinita, Shield Advanced si configura CloudWatch per avvisare l'utente dopo un

solo indicatore di un potenziale evento DDoS. Se necessario, puoi utilizzare la CloudWatch console per modificare questa impostazione in modo da avvisarti solo dopo il rilevamento di più indicatori.

> **Note**
>
> Oltre agli allarmi, puoi anche utilizzare una CloudWatch dashboard per monitorare le potenziali attività DDoS. La dashboard raccoglie ed elabora i dati grezzi di Shield Advanced in metriche leggibili e quasi in tempo reale. Puoi utilizzare le statistiche in Amazon CloudWatch per avere una prospettiva sulle prestazioni della tua applicazione o del tuo servizio web. Per ulteriori informazioni, consulta Cosa c'è CloudWatch nella Amazon CloudWatch User Guide. Per istruzioni sulla creazione di una CloudWatch dashboard, consultaMonitoraggio con Amazon CloudWatch. Per informazioni su metriche specifiche di Shield Advanced che puoi aggiungere alla dashboard, consultaAWS Shield Advanced metriche.

Una volta completata la configurazione di Shield Advanced, acquisisci familiarità con le opzioni disponibili per la visualizzazione degli eventi su. Visibilità sugli eventi DDoS

Guida introduttiva alle policy dei gruppi di sicurezza di AWS Firewall Manager Amazon VPC

AWS Firewall Manager Per abilitare i gruppi di sicurezza Amazon VPC in tutta l'organizzazione, esegui i seguenti passaggi in sequenza.

Argomenti

- Fase 1: completamento dei prerequisiti
- Fase 2: Crea un gruppo di sicurezza Amazon VPC da utilizzare nella tua policy
- Fase 3: Creare e applicare una politica di gruppo di sicurezza comune

Fase 1: completamento dei prerequisiti

Vi sono diversi passaggi obbligatori per preparare l'account AWS Firewall Manager. Tali fasi sono descritte nell'articolo AWS Firewall Manager prerequisiti. Completare tutti i prerequisiti prima di passare a Fase 2: Crea un gruppo di sicurezza Amazon VPC da utilizzare nella tua policy.

Fase 2: Crea un gruppo di sicurezza Amazon VPC da utilizzare nella tua policy

In questo passaggio, crei un gruppo di sicurezza da applicare all'intera organizzazione utilizzando Firewall Manager.

> **Note**
>
> Per questa esercitazione, non si applicano i criteri del gruppo di protezione alle risorse dell'organizzazione. È sufficiente creare il criterio e vedere cosa accadrebbe se si applicasse il gruppo di sicurezza del criterio alle risorse. A tale scopo, disabilitare la correzione automatica del criterio.

Se è già stato definito un gruppo di sicurezza generale, ignorare questo passaggio e andare a Fase 3: Creare e applicare una politica di gruppo di sicurezza comune.

Per creare un gruppo di sicurezza da utilizzare in una politica di gruppo di sicurezza comune di Firewall Manager

- Crea un gruppo di sicurezza da applicare a tutti gli account e le risorse della tua organizzazione, seguendo le indicazioni riportate nella sezione Security Groups for Your VPC nella Amazon VPC User Guide.

  Per informazioni sulle opzioni delle regole dei gruppi di protezione, vedere Riferimento alle regole del gruppo di sicurezza.

È possibile ora procedere a Fase 3: Creare e applicare una politica di gruppo di sicurezza comune.

Fase 3: Creare e applicare una politica di gruppo di sicurezza comune

Dopo aver completato i prerequisiti, si crea una politica di gruppo di sicurezza AWS Firewall Manager comune. Una politica di gruppo di sicurezza comune fornisce un gruppo di sicurezza controllato centralmente per l'intera AWS organizzazione. Definisce inoltre le risorse Account AWS e le risorse a cui si applica il gruppo di sicurezza. Oltre alle politiche comuni dei gruppi di sicurezza, Firewall Manager supporta le politiche dei gruppi di sicurezza per il controllo dei contenuti, per gestire le regole dei gruppi di sicurezza in uso nell'organizzazione, e le politiche dei gruppi di sicurezza per il controllo dell'utilizzo, per gestire i gruppi di sicurezza inutilizzati e ridondanti. Per ulteriori informazioni, consulta Politiche dei gruppi di sicurezza.

Per questa esercitazione, è possibile creare un criterio di gruppo di protezione comune e impostarne l'azione in modo da non correggere automaticamente. Ciò consente di vedere quali effetti avrebbe la politica senza apportare modifiche all'organizzazione. AWS

Per creare una politica di gruppo di sicurezza comune di Firewall Manager (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Se i prerequisiti non sono stati soddisfatti, la console visualizzerà le istruzioni su come risolvere eventuali problemi. Seguire le istruzioni e quindi tornare a questo passaggio per creare un criterio di gruppo di protezione comune.
4. Scegli Crea policy.
5. Per Tipo di criterio, scegliere Gruppo di protezione.
6. Per Tipo di criteri di gruppo di protezione, scegliere Gruppi di protezione comuni.
7. Per Regione, scegli un Regione AWS.
8. Seleziona Successivo.
9. Per Nome della politica, inserisci un nome descrittivo.
10. Le regole dei criteri consentono di scegliere la modalità di applicazione e gestione dei gruppi di protezione in questo criterio. Per questo tutorial, lascia deselezionate le opzioni.
11. Scegliere Aggiungi gruppo di sicurezza primario, selezionare il gruppo di protezione creato per questa esercitazione e scegliere Aggiungi gruppo di sicurezza.
12. Per Azione Criteri, scegliere Identificare risorse che non sono conformi alle regole dei criteri, ma non eseguire la correzione automatica.
13. Seleziona Successivo.

14. Account AWS interessati da questa politica ti consente di restringere l'ambito della tua politica specificando gli account da includere o escludere. Per questa esercitazione, scegliere Includi tutti gli account nell'organizzazione.
15. Per Tipo di risorsa, scegli uno o più tipi, in base alle risorse che hai definito per la tua AWS organizzazione.
16. Risorse consente di restringere l'ambito dei criteri specificando i tag risorsa per l'inclusione o l'esclusione. Per utilizzare il tag, è necessario innanzitutto etichettare le risorse. Per ulteriori informazioni sull'assegnazione di tag alle risorse, vedere Utilizzo dell'editor dei tag. Per questa esercitazione, scegliere Includi tutte le risorse corrispondenti al tipo di risorsa selezionato.
17. Seleziona Successivo.
18. Rivedere le impostazioni dei criteri. Verificare che le azioni dei criteri siano impostate su Identificare le risorse che non sono conformi alle regole dei criteri, ma che non vengano corrette automaticamente. In questo modo è possibile esaminare le modifiche apportate dal criterio, senza apportare modifiche al momento.
19. Scegli Crea policy.

    Nel riquadro delle AWS Firewall Manager politiche, la tua politica dovrebbe essere elencata. Probabilmente indicherà In sospeso sotto le intestazioni degli account e indicherà che la correzione automatica è disabilitata. La creazione di una politica può richiedere diversi minuti. Dopo aver sostituito lo stato In sospeso con il conteggio degli account, è possibile scegliere il nome del criterio per esplorare lo stato di conformità degli account e delle risorse. Per informazioni, consultare, Visualizzazione delle informazioni sulla conformità per una AWS Firewall Manager politica
20. Al termine dell'esplorazione, se non si desidera mantenere il criterio creato per questa esercitazione, scegliere il nome del criterio, scegliere Elimina, scegliere Pulisci risorse create da questo criterio e infine Elimina

Per ulteriori informazioni sui criteri dei gruppi di sicurezza di Firewall Manager, vederePolitiche dei gruppi di sicurezza.

Guida introduttiva alle AWS Firewall ManagerAWS Network Firewall politiche

AWS Firewall Manager Per attivare un firewall AWS Network Firewall in tutta l'organizzazione, esegui i seguenti passaggi in sequenza. Per informazioni sulle politiche del firewall di rete di Firewall Manager, vedereAWS Network Firewall politiche.

Argomenti

Fase 1: Completare i prerequisiti generali

Vi sono diversi passaggi obbligatori per preparare l'account AWS Firewall Manager. Tali fasi sono descritte nell'articolo AWS Firewall Manager prerequisiti. Completa tutti i prerequisiti prima di procedere al passaggio successivo.

Fase 2: Creare un gruppo di regole Network Firewall da utilizzare nella policy

Per seguire questo tutorial, è necessario conoscere AWS Network Firewall e configurare i gruppi di regole e le politiche del firewall.

È necessario disporre di almeno un gruppo di regole in Network Firewall che verrà utilizzato nella AWS Firewall Manager politica. Se non hai già creato un gruppo di regole in Network Firewall, fallo ora. Per informazioni sull'utilizzo di Network Firewall, consulta la Guida per AWS Network Firewall gli sviluppatori.

Fase 3: Creare e applicare una policy Network Firewall

Dopo aver completato i prerequisiti, si crea una politica AWS Firewall Manager Network Firewall. Una policy Network Firewall fornisce un AWS Network Firewall firewall controllato centralmente per l'intera AWS organizzazione. Definisce inoltre le risorse Account AWS e le risorse a cui si applica il firewall.

Per ulteriori informazioni su come Firewall Manager gestisce le politiche del Network Firewall, vedereAWS Network Firewall politiche.

Per creare una politica Firewall Manager Network Firewall (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

> **Note**
>
> Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Se non hai soddisfatto i prerequisiti, la console visualizza le istruzioni su come risolvere eventuali problemi. Segui le istruzioni, quindi torna a questo passaggio per creare una politica Network Firewall.
4. Scegli Crea politica di sicurezza.
5. Per Policy type (Tipo di policy), scegliere AWS Network Firewall.
6. Per Regione, scegli un Regione AWS.
7. Seleziona Successivo.
8. Per Nome della politica, inserisci un nome descrittivo.
9. La configurazione della politica consente di definire la politica del firewall. Si tratta dello stesso processo utilizzato nella AWS Network Firewall console. Aggiungi i gruppi di regole che desideri utilizzare nella tua politica e fornisci le azioni stateless predefinite. Per questo tutorial, configura questa politica come faresti con una politica firewall in Network Firewall.

> **Note**
>
> La riparazione automatica viene eseguita automaticamente per le politiche del AWS Firewall Manager Network Firewall, quindi qui non è disponibile un'opzione per scegliere di non eseguire la riparazione automatica.

10. Seleziona Successivo.
11. Per gli endpoint firewall, scegli Endpoint firewall multipli. Questa opzione offre un'elevata disponibilità per il firewall. Quando si crea la policy, Firewall Manager crea una sottorete firewall in ogni zona di disponibilità in cui sono presenti sottoreti pubbliche da proteggere.
12. Per la configurazione delle AWS Network Firewall route, scegli Monitor per fare in modo che Firewall Manager monitori i tuoi VPC per rilevare eventuali violazioni della configurazione delle route e ti avvisi con suggerimenti di correzione per aiutarti a rendere le route conformi. Facoltativamente, se non desideri che le configurazioni delle rotte vengano monitorate da Firewall Manager e ricevere questi avvisi, scegli Disattivato.

> **Note**
>
> Il monitoraggio fornisce dettagli sulle risorse non conformi a causa di una configurazione errata del percorso e suggerisce azioni correttive dall'API Firewall Manager. `GetViolationDetails` Ad esempio, Network Firewall ti avvisa se il traffico non viene instradato attraverso gli endpoint firewall creati dalla tua policy.

> **Warning**
>
> Se scegli Monitor, non potrai modificarlo su Off in futuro per la stessa politica. È necessario creare una nuova politica.

13. Per Tipo di traffico, seleziona Aggiungi alla politica del firewall per indirizzare il traffico attraverso il gateway Internet.
14. Account AWS interessati da questa politica consente di restringere l'ambito della politica specificando gli account da includere o escludere. Per questa esercitazione, scegliere Includi tutti gli account nell'organizzazione.
15. Il tipo di risorsa per una policy Network Firewall è sempre VPC.
16. Risorse consente di restringere l'ambito dei criteri specificando i tag risorsa per l'inclusione o l'esclusione. Per utilizzare il tag, è necessario innanzitutto etichettare le risorse. Per ulteriori informazioni sull'assegnazione di tag alle risorse, vedere Utilizzo dell'editor dei tag. Per questa esercitazione, scegliere Includi tutte le risorse corrispondenti al tipo di risorsa selezionato.
17. Seleziona Successivo.
18. Controlla le impostazioni della politica, quindi scegli Crea politica.

    Nel riquadro delle AWS Firewall Manager politiche, la tua politica dovrebbe essere elencata. La creazione di una politica può richiedere diversi minuti. Fino al completamento del processo di creazione, la politica indica che è in sospeso. Quando la policy è pronta, lo stato si aggiorna con il numero di account inclusi nell'ambito. Puoi scegliere il nome della politica per esplorare lo stato di conformità degli account e delle risorse. Per informazioni, consultare, Visualizzazione delle informazioni sulla conformità per una AWS Firewall Manager politica
19. Al termine dell'esplorazione, se non desideri mantenere la politica creata per questo tutorial, scegli il nome della politica, scegli Elimina, scegli Pulisci le risorse create da questa politica. e infine scegli Elimina.

Per ulteriori informazioni sulle politiche del firewall di rete di Firewall Manager, vedereAWS Network Firewall politiche.

Guida introduttiva alle AWS Firewall Manager politiche del firewall DNS

AWS Firewall Manager Per abilitare Amazon Route 53 Resolver DNS Firewall in tutta l'organizzazione, esegui i seguenti passaggi in sequenza. Per informazioni sulle politiche del firewall DNS di Firewall Manager, vederePolitiche del firewall DNS di Amazon Route 53 Resolver.

Argomenti

- Fase 1: Completare i prerequisiti generali
- Fase 2: Creare i gruppi di regole del firewall DNS da utilizzare nella policy
- Fase 3: Creare e applicare una policy DNS Firewall

Fase 1: Completare i prerequisiti generali

Vi sono diversi passaggi obbligatori per preparare l'account AWS Firewall Manager. Tali fasi sono descritte nell'articolo AWS Firewall Manager prerequisiti. Completa tutti i prerequisiti prima di procedere al passaggio successivo.

Fase 2: Creare i gruppi di regole del firewall DNS da utilizzare nella policy

Per seguire questo tutorial, è necessario conoscere il firewall DNS di Amazon Route 53 Resolver e sapere come configurarne i gruppi di regole.

È necessario disporre di almeno un gruppo di regole in DNS Firewall da utilizzare nella politica. AWS Firewall Manager Se non hai già creato un gruppo di regole in DNS Firewall, fallo ora. Per informazioni sull'uso di DNS Firewall, consulta Amazon Route 53 Resolver DNS Firewall nella Amazon Route 53 Developer Guide.

Fase 3: Creare e applicare una policy DNS Firewall

Dopo aver completato i prerequisiti, si crea una policy AWS Firewall Manager DNS Firewall. Una policy DNS Firewall fornisce una serie di associazioni di gruppi di regole DNS Firewall controllate centralmente per l'intera organizzazione. AWS Definisce inoltre le risorse Account AWS e le risorse a cui si applica il firewall.

Per ulteriori informazioni su come Firewall Manager gestisce le associazioni dei gruppi di regole del firewall DNS, vederePolitiche del firewall DNS di Amazon Route 53 Resolver.

Per creare una policy Firewall DNS Firewall Manager (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.
2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Se non hai soddisfatto i prerequisiti, la console visualizza le istruzioni su come risolvere eventuali problemi. Segui le istruzioni, quindi torna a questo passaggio per creare una policy DNS Firewall.
4. Scegli Crea politica di sicurezza.
5. Per il tipo di policy, scegli Amazon Route 53 Resolver DNS Firewall.
6. Per Regione, scegli un. Regione AWS
7. Seleziona Successivo.
8. Per Nome della politica, inserisci un nome descrittivo.
9. La configurazione delle policy consente di definire le associazioni dei gruppi di regole del firewall DNS che si desidera gestire da Firewall Manager. Aggiungi i gruppi di regole che desideri utilizzare nella tua politica. Puoi definire un'associazione da valutare prima per i tuoi VPC e un'altra da valutare per ultima. Per questo tutorial, aggiungi una o due associazioni di gruppi di regole, a seconda delle tue esigenze.
10. Seleziona Successivo.
11. Account AWS interessati da questa politica consente di restringere l'ambito della politica specificando gli account da includere o escludere. Per questa esercitazione, scegliere Includi tutti gli account nell'organizzazione.
12. Il tipo di risorsa per una politica del firewall DNS è sempre VPC.
13. Risorse consente di restringere l'ambito dei criteri specificando i tag risorsa per l'inclusione o l'esclusione. Per utilizzare il tag, è necessario innanzitutto etichettare le risorse. Per ulteriori informazioni sull'assegnazione di tag alle risorse, vedere Utilizzo dell'editor dei tag. Per questa esercitazione, scegliere Includi tutte le risorse corrispondenti al tipo di risorsa selezionato.
14. Seleziona Successivo.
15. Controlla le impostazioni della policy, quindi scegli Crea policy.

    Nel riquadro delle AWS Firewall Manager politiche, la tua politica dovrebbe essere elencata. La creazione di una politica può richiedere diversi minuti. Fino al completamento del processo di creazione, la politica indica che è in sospeso. Quando la policy è pronta, lo stato si aggiorna con

il numero di account inclusi nell'ambito. Puoi scegliere il nome della politica per esplorare lo stato di conformità degli account e delle risorse. Per informazioni, consultare, Visualizzazione delle informazioni sulla conformità per una AWS Firewall Manager politica

16. Al termine dell'esplorazione, se non desideri mantenere la politica creata per questo tutorial, scegli il nome della politica, scegli Elimina, scegli Pulisci le risorse create da questa politica. e infine scegli Elimina.

Per ulteriori informazioni sulle politiche del firewall DNS di Firewall Manager, vederePolitiche del firewall DNS di Amazon Route 53 Resolver.

Guida introduttiva alle policy di AWS Firewall Manager Palo Alto Networks Cloud Next Generation Firewall

AWS Firewall Manager Per abilitare le politiche Palo Alto Networks Cloud Next Generation Firewall (NGFW), esegui i seguenti passaggi in sequenza. Per informazioni sulle politiche NGFW di Palo Alto Networks Cloud, vedere. Politiche NGFW di Palo Alto Networks Cloud

Argomenti

- Fase 1: Completare i prerequisiti generali
- Fase 2: Completare i prerequisiti della policy NGFW di Palo Alto Networks Cloud
- Fase 3: Creare e applicare una policy NGFW di Palo Alto Networks Cloud

Fase 1: Completare i prerequisiti generali

Vi sono diversi passaggi obbligatori per preparare l'account AWS Firewall Manager. Tali fasi sono descritte nell'articolo AWS Firewall Manager prerequisiti. Completa tutti i prerequisiti prima di procedere al passaggio successivo.

Fase 2: Completare i prerequisiti della policy NGFW di Palo Alto Networks Cloud

Ci sono un paio di passaggi obbligatori aggiuntivi che è necessario completare per utilizzare le policy NGFW di Palo Alto Networks Cloud. Tali fasi sono descritte nell'articolo Prerequisiti della policy Palo Alto Networks Cloud Next Generation Firewall. Completa tutti i prerequisiti prima di procedere al passaggio successivo.

Fase 3: Creare e applicare una policy NGFW di Palo Alto Networks Cloud

Dopo aver completato i prerequisiti, si crea una policy NGFW di AWS Firewall Manager Palo Alto Networks Cloud.

Per ulteriori informazioni sulle politiche di Firewall Manager per Palo Alto Networks Cloud NGFW, vedere. Politiche NGFW di Palo Alto Networks Cloud

Per creare una policy Firewall Manager per Palo Alto Networks Cloud NGFW (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Scegli Crea policy.
4. Per il tipo di policy, scegli Palo Alto Networks Cloud NGFW. Se non ti sei ancora abbonato al servizio Palo Alto Networks Cloud NGFW nel AWS Marketplace, devi prima farlo. Per iscriverti al AWS Marketplace, scegli Visualizza i dettagli del AWS Marketplace.
5. Per il modello di implementazione, scegli il modello distribuito o il modello centralizzato. Il modello di distribuzione determina il modo in cui Firewall Manager gestisce gli endpoint per la policy. Con il modello distribuito, Firewall Manager mantiene gli endpoint del firewall in ogni VPC che rientra nell'ambito delle policy. Con il modello centralizzato, Firewall Manager mantiene un singolo endpoint in un VPC di ispezione.
6. Per Regione, scegli un. Regione AWS Per proteggere le risorse in più regioni, devi creare politiche separate per ogni regione.
7. Seleziona Successivo.
8. Per Nome della politica, inserisci un nome descrittivo.
9. Nella configurazione della policy, scegli la policy firewall NGFW di Palo Alto Networks Cloud da associare a questa policy. L'elenco delle politiche firewall NGFW di Palo Alto Networks Cloud

contiene tutte le politiche firewall Palo Alto Networks Cloud NGFW associate al tenant Palo Alto Networks Cloud NGFW. Per informazioni sulla creazione e la gestione delle policy firewall Palo Alto Networks Cloud NGFW, consulta la sezione Deploy Palo Alto Networks Cloud NGFW per l'argomento della guida all'implementazione di Palo Alto Networks Cloud NGFW. AWS AWS Firewall Manager AWS

10. Per la registrazione NGFW di Palo Alto Networks Cloud: opzionale, scegli facoltativamente quali tipi di log Palo Alto Networks Cloud NGFW registrare per la tua politica. Per informazioni sui tipi di log NGFW di Palo Alto Networks Cloud, consulta Configura la registrazione per Palo Alto Networks Cloud NGFW nella guida all'implementazione di Palo Alto Networks Cloud NGFW. AWS AWS

    Per la destinazione dei log, specificare in che momento Firewall Manager deve scrivere i log.

11. Seleziona Successivo.
12. In Configura un endpoint firewall di terze parti, esegui una delle seguenti operazioni, a seconda che utilizzi il modello di distribuzione distribuito o centralizzato per creare gli endpoint firewall:

    - Se utilizzi il modello di distribuzione distribuito per questa politica, in Zone di disponibilità, seleziona in quali zone di disponibilità creare gli endpoint del firewall. È possibile selezionare le zone di disponibilità in base al nome della zona di disponibilità o all'ID della zona di disponibilità.
    - Se utilizzi il modello di distribuzione centralizzato per questa policy, nella configurazione degli AWS Firewall Manager endpoint in configurazione Inspection VPC, inserisci l'ID AWS account del proprietario del VPC di ispezione e l'ID VPC del VPC di ispezione.
        - In Zone di disponibilità, seleziona le zone di disponibilità in cui creare gli endpoint del firewall. È possibile selezionare le zone di disponibilità in base al nome della zona di disponibilità o all'ID della zona di disponibilità.
13. Seleziona Successivo.
14. Per l'ambito della politica, in base a cui si applica Account AWS questa politica, scegli l'opzione seguente:

    - Se desideri applicare la politica a tutti gli account della tua organizzazione, lascia la selezione predefinita Includi tutti gli account della mia AWS organizzazione.
    - Se desideri applicare la politica solo a conti specifici o account appartenenti a unità AWS Organizations organizzative (OU) specifiche, scegli Includi solo gli account e le unità organizzative specificati, quindi aggiungi gli account e le unità organizzative che desideri includere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità

organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

- Se desideri applicare la politica a tutti i conti o le unità AWS Organizations organizzative (OU) tranne uno specifico, scegli Escludi gli account e le unità organizzative specificati e includi tutti gli altri, quindi aggiungi gli account e le unità organizzative che desideri escludere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

È possibile scegliere solo una delle opzioni.

Dopo aver applicato la policy, Firewall Manager valuta automaticamente tutti i nuovi account in base alle impostazioni dell'utente. Ad esempio, se includi solo account specifici, Firewall Manager non applica la politica a nessun nuovo account. Come altro esempio, se si include un'unità organizzativa, quando si aggiunge un account all'unità organizzativa o a una delle relative unità organizzative secondarie, Firewall Manager applica automaticamente la politica al nuovo account.

15. Il tipo di risorsa per le politiche del Network Firewall è VPC.
16. In Resources (Risorse), se si desidera proteggere (o escludere) solo le risorse con tag specifici, selezionare l'opzione appropriata, quindi immettere i tag da includere o escludere. È possibile scegliere una sola opzione. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .

    Se si immettono più tag, una risorsa deve avere tutti i tag da includere o escludere.
17. Per Concedi l'accesso a più account, scegli Scarica AWS CloudFormation modello. In questo modo viene scaricato un AWS CloudFormation modello che puoi utilizzare per creare uno AWS CloudFormation stack. Questo stack crea un AWS Identity and Access Management ruolo che concede a Firewall Manager le autorizzazioni per più account per gestire le risorse NGFW di Palo Alto Networks Cloud. Per informazioni sugli stack, consulta Working with stacks nella Guida per l'utente.AWS CloudFormation
18. Seleziona Successivo.
19. Per i tag Policy, aggiungi tutti i tag identificativi che desideri per la policy di Firewall Manager. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .
20. Seleziona Successivo.

21. Rivedere la nuova policy. Per apportare eventuali modifiche, scegliere Edit (Modifica) nell'area che si desidera modificare. In questo modo si torna al passaggio corrispondente della creazione guidata. Al termine, scegliere Create policy (Crea policy).

Per ulteriori informazioni sulle politiche NGFW di Firewall Manager Palo Alto Networks Cloud, vedere. Politiche NGFW di Palo Alto Networks Cloud

Guida introduttiva alle politiche di AWS Firewall Manager Fortigate CNF

Fortigate Cloud Native Firewall (CNF) as a Service è un servizio firewall di terze parti che puoi utilizzare per le tue politiche. AWS Firewall Manager Con Fortigate CNF for Firewall Manager, puoi creare e distribuire centralmente risorse e set di policy Fortigate CNF su tutti i tuoi account. AWS Per abilitare le policy AWS Firewall Manager CNF di Fortigate, esegui i seguenti passaggi in sequenza. Per ulteriori informazioni sulle politiche CNF di Fortigate, vedere. Politiche di Fortigate Cloud Native Firewall (CNF) as a Service

Argomenti

- Fase 1: Completare i prerequisiti generali
- Fase 2: Completare i prerequisiti della policy Fortigate CNF
- Fase 3: Creare e applicare una policy Fortigate CNF

Fase 1: Completare i prerequisiti generali

Vi sono diversi passaggi obbligatori per preparare l'account AWS Firewall Manager. Tali fasi sono descritte nell'articolo AWS Firewall Manager prerequisiti. Completa tutti i prerequisiti prima di procedere al passaggio successivo.

Fase 2: Completare i prerequisiti della policy Fortigate CNF

Esistono ulteriori passaggi obbligatori che è necessario completare per utilizzare le politiche CNF di Fortigate. Tali fasi sono descritte nell'articolo Prerequisiti della politica Fortigate Cloud Native Firewall (CNF) as a Service. Completa tutti i prerequisiti prima di procedere al passaggio successivo.

Fase 3: Creare e applicare una policy Fortigate CNF

Dopo aver completato i prerequisiti, crei una AWS Firewall Manager policy Fortigate CNF.

Per ulteriori informazioni sulle politiche di Firewall Manager per Fortigate CNF, vedere. Politiche di Fortigate Cloud Native Firewall (CNF) as a Service

Per creare una policy Firewall Manager per Fortigate CNF (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Scegli Crea policy.
4. Per il tipo di policy, scegli Fortigate CNF. Se non ti sei ancora abbonato al servizio Fortigate CNF nel AWS Marketplace, devi prima farlo. Per iscriverti al AWS Marketplace, scegli Visualizza i dettagli del AWS Marketplace.
5. Per il modello di implementazione, scegli il modello distribuito o il modello centralizzato. Il modello di distribuzione determina il modo in cui Firewall Manager gestisce gli endpoint per la policy. Con il modello distribuito, Firewall Manager mantiene gli endpoint del firewall in ogni VPC che rientra nell'ambito delle policy. Con il modello centralizzato, Firewall Manager mantiene un singolo endpoint in un VPC di ispezione.
6. Per Regione, scegli un. Regione AWS Per proteggere le risorse in più regioni, devi creare politiche separate per ogni regione.
7. Seleziona Successivo.
8.
9. Nella configurazione della politica, scegli la politica firewall Fortigate CNF da associare a questa politica. L'elenco delle politiche firewall di Fortigate CNF contiene tutte le politiche firewall Fortigate CNF associate al tenant di Fortigate CNF. Per informazioni sulla creazione e la gestione delle politiche firewall di Fortigate CNF, consulta la documentazione di Fortigate CNF.
10. Seleziona Successivo.
11. In Configura un endpoint firewall di terze parti, esegui una delle seguenti operazioni, a seconda che utilizzi il modello di distribuzione distribuito o centralizzato per creare gli endpoint firewall:

- Se utilizzi il modello di distribuzione distribuito per questa politica, in Zone di disponibilità, seleziona in quali zone di disponibilità creare gli endpoint del firewall. È possibile selezionare le zone di disponibilità in base al nome della zona di disponibilità o all'ID della zona di disponibilità.
- Se utilizzi il modello di distribuzione centralizzato per questa policy, nella configurazione degli AWS Firewall Manager endpoint in configurazione Inspection VPC, inserisci l'ID AWS account del proprietario del VPC di ispezione e l'ID VPC del VPC di ispezione.
  - In Zone di disponibilità, seleziona le zone di disponibilità in cui creare gli endpoint del firewall. È possibile selezionare le zone di disponibilità in base al nome della zona di disponibilità o all'ID della zona di disponibilità.

12. Seleziona Successivo.
13. Per l'ambito della politica, in base a cui si applica Account AWS questa politica, scegli l'opzione seguente:

    - Se desideri applicare la politica a tutti gli account della tua organizzazione, lascia la selezione predefinita Includi tutti gli account della mia AWS organizzazione.
    - Se desideri applicare la politica solo a conti specifici o account appartenenti a unità AWS Organizations organizzative (OU) specifiche, scegli Includi solo gli account e le unità organizzative specificati, quindi aggiungi gli account e le unità organizzative che desideri includere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.
    - Se desideri applicare la politica a tutti i conti o le unità AWS Organizations organizzative (OU) tranne uno specifico, scegli Escludi gli account e le unità organizzative specificati e includi tutti gli altri, quindi aggiungi gli account e le unità organizzative che desideri escludere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

    È possibile scegliere solo una delle opzioni.

    Dopo aver applicato la policy, Firewall Manager valuta automaticamente tutti i nuovi account in base alle impostazioni dell'utente. Ad esempio, se includi solo account specifici, Firewall Manager non applica la politica a nessun nuovo account. Come altro esempio, se si include un'unità organizzativa, quando si aggiunge un account all'unità organizzativa o a una delle

relative unità organizzative secondarie, Firewall Manager applica automaticamente la politica al nuovo account.

14. Il tipo di risorsa per le politiche del Network Firewall è VPC.
15. In Resources (Risorse), se si desidera proteggere (o escludere) solo le risorse con tag specifici, selezionare l'opzione appropriata, quindi immettere i tag da includere o escludere. È possibile scegliere una sola opzione. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .

    Se si immettono più tag, una risorsa deve avere tutti i tag da includere o escludere.
16. Per Concedi l'accesso a più account, scegli Scarica AWS CloudFormation modello. In questo modo viene scaricato un AWS CloudFormation modello che puoi utilizzare per creare uno AWS CloudFormation stack. Questo stack crea un AWS Identity and Access Management ruolo che concede a Firewall Manager le autorizzazioni per più account per gestire le risorse Fortigate CNF. Per informazioni sugli stack, consulta Working with stacks nella Guida per l'utente.AWS CloudFormation Per creare uno stack, è necessario l'ID dell'account dal portale Fortigate CNF.
17. Seleziona Successivo.
18. Per i tag Policy, aggiungi tutti i tag identificativi che desideri per la policy di Firewall Manager. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .
19. Seleziona Successivo.
20. Rivedere la nuova policy. Per apportare eventuali modifiche, scegliere Edit (Modifica) nell'area che si desidera modificare. In questo modo si torna al passaggio corrispondente della creazione guidata. Al termine, scegliere Create policy (Crea policy).

Per ulteriori informazioni sulle politiche CNF di Firewall Manager Fortigate, vedere. Politiche di Fortigate Cloud Native Firewall (CNF) as a Service

Lavorare con AWS Firewall Manager le politiche

AWS Firewall Manager fornisce i seguenti tipi di politiche:

- AWS WAFpolicy — Firewall Manager supporta le policy AWS WAF classiche AWS WAF e le policy. Per entrambe le versioni, è possibile definire quali risorse sono protette dalla policy.
  - Per quanto riguarda la AWS WAF policy, è possibile definire un set di gruppi di regole da eseguire per primi nell'ACL Web e un set di gruppi di regole da eseguire per ultimi. Negli account

a cui si applica l'ACL Web, il proprietario dell'account può aggiungere regole e gruppi di regole da eseguire tra i due set di gruppi di regole di Firewall Manager.

  - Per AWS WAF Classic, si crea una politica che definisce un singolo gruppo di regole.
- Politica Shield Advanced: questa politica applica la AWS Shield Advanced protezione a determinati account e risorse.
- Policy di gruppo di sicurezza di Amazon VPC: questo tipo di policy ti dà il controllo sui gruppi di sicurezza utilizzati in tutta l'organizzazione AWS Organizations e ti consente di applicare un set di regole di base all'interno dell'organizzazione.
- Politica Network Firewall: questa politica applica AWS Network Firewall la protezione ai VPC dell'organizzazione.
- Policy firewall DNS di Amazon Route 53 Resolver: questa politica applica le protezioni DNS Firewall ai VPC della tua organizzazione.
- Policy firewall di terze parti: questa politica applica protezioni firewall di terze parti. I firewall di terze parti sono disponibili in abbonamento tramite la console AWS Marketplace su AWS Marketplace.
  - Policy NGFW di Palo Alto Networks Cloud: questa policy applica le protezioni Palo Alto Networks Cloud Next Generation Firewall (NGFW) e gli stack di regole Palo Alto Networks Cloud NGFW ai VPC dell'organizzazione.
  - Policy Fortigate Cloud Native Firewall (CNF) as a Service: questa policy applica le protezioni di Fortigate Cloud Native Firewall (CNF) as a Service. Fortigate CNF è una soluzione incentrata sul cloud che blocca le minacce Zero-Day e protegge le infrastrutture cloud con la prevenzione avanzata delle minacce leader del settore, firewall intelligenti per applicazioni web (WAF) e protezione delle API.

Una policy di Firewall Manager è specifica per ogni tipo di policy. Se si desidera applicare più tipi di criteri tra gli account, è possibile creare più criteri. È possibile creare più criteri per ogni tipo.

Se si aggiunge un nuovo account a un'organizzazione con cui è stato creato AWS Organizations, Firewall Manager applica automaticamente la politica alle risorse di quell'account che rientrano nell'ambito della politica.

Impostazioni generali per AWS Firewall Manager le politiche

AWS Firewall Manager le politiche gestite hanno alcune impostazioni e comportamenti comuni. Per tutti, è necessario specificare un nome e definire l'ambito della politica e utilizzare l'etichettatura delle risorse per controllare l'ambito della politica. È possibile scegliere di visualizzare gli account e le

risorse non conformi senza intraprendere azioni correttive o di correggere automaticamente le risorse non conformi.

Per informazioni sull'ambito della politica, vedereAWS Firewall Manager ambito della politica.

Creazione di una AWS Firewall Manager politica

I passaggi per la creazione di un criterio variano a seconda dei diversi tipi di criteri. Assicurarsi di utilizzare la procedura per il tipo di criterio necessario.

> **Important**
>
> AWS Firewall Manager non supporta Amazon Route 53 o AWS Global Accelerator. Se desideri proteggere queste risorse con Shield Advanced, non puoi utilizzare una policy Firewall Manager. Seguire invece le istruzioni in Aggiungere AWS Shield Advanced protezione alle risorse AWS.

Argomenti

- Creazione di una AWS Firewall Manager politica per AWS WAF
- Creazione di una AWS Firewall Manager politica per AWS WAF Classic
- Creazione di una AWS Firewall Manager politica per AWS Shield Advanced
- Creazione di una policy di gruppo di sicurezza comune AWS Firewall Manager
- Creazione di una policy di gruppo di sicurezza di controllo del contenuto AWS Firewall Manager
- Creazione di una policy di gruppo di sicurezza di controllo dell'utilizzo AWS Firewall Manager
- Creazione di una AWS Firewall Manager politica per AWS Network Firewall
- Creazione di una AWS Firewall Manager policy per Amazon Route 53 Resolver DNS Firewall
- Creazione di una AWS Firewall Manager policy per Palo Alto Networks Cloud NGFW
- Creazione di una AWS Firewall Manager policy per Fortigate Cloud Native Firewall (CNF) as a Service

Creazione di una AWS Firewall Manager politica per AWS WAF

In una AWS WAF politica di Firewall Manager, puoi utilizzare gruppi di regole gestiti, che AWS e Marketplace AWS i venditori creano e gestiscono per te. È inoltre possibile creare e utilizzare propri gruppi di regole. Per ulteriori informazioni sui gruppi di regole, consulta Gruppi di regole.

Se desideri utilizzare i tuoi gruppi di regole, creali prima di creare la AWS WAF policy di Firewall Manager. Per le linee guida, consulta Gestione dei propri gruppi di regole. Per utilizzare una singola regola personalizzata, è necessario definire il proprio gruppo di regole, definire la regola all'interno del gruppo e quindi utilizzare il gruppo di regole nella policy.

Per informazioni sulle AWS WAF politiche di Firewall Manager, vedereAWS WAF politiche.

Per creare una policy Firewall Manager per AWS WAF (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Scegli Crea policy.
4. Per Policy type (Tipo di policy), scegliere AWS WAF.
5. Per Regione, scegli un Regione AWS. Per proteggere le CloudFront distribuzioni Amazon, scegli Global.

   Per proteggere le risorse in più regioni (diverse dalle CloudFront distribuzioni), è necessario creare policy Firewall Manager separate per ogni regione.
6. Seleziona Successivo.
7. Per Nome della politica, inserire un nome descrittivo. Firewall Manager include il nome della policy nei nomi degli ACL Web che gestisce. I nomi degli ACL Web sono `FMManagedWebACLV2-` seguiti dal nome della policy immesso qui e dal timestamp di creazione degli ACL Web-, in millisecondi UTC. Ad esempio, `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`.
8. Per l'ispezione del corpo su richiesta Web, puoi modificare facoltativamente il limite di dimensione del corpo. Per informazioni sui limiti di dimensioni per l'ispezione delle carrozzerie, comprese le considerazioni relative ai prezzi, consultate la Gestione dei limiti di dimensione delle ispezioni corporee Guida per gli AWS WAF sviluppatori.

9. In Policy rules, aggiungi i gruppi di regole che desideri valutare AWS WAF per primi e per ultimi nell'ACL web. Per utilizzare il controllo delle versioni AWS WAF gestito dei gruppi di regole, attiva Abilita il controllo delle versioni. I singoli responsabili dell'account possono aggiungere regole e gruppi di regole tra i primi gruppi di regole e gli ultimi gruppi di regole. Per ulteriori informazioni sull'utilizzo dei gruppi di AWS WAF regole nelle politiche di Firewall Manager per AWS WAF, vedereAWS WAF politiche.

   (Facoltativo) Per personalizzare il modo in cui l'ACL Web utilizza il gruppo di regole, scegli Modifica. Di seguito sono riportate le impostazioni di personalizzazione più comuni:

   - Per i gruppi di regole gestiti, sostituisci le azioni delle regole per alcune o tutte le regole. Se non si definisce un'azione di sostituzione per una regola, la valutazione utilizza l'azione della regola definita all'interno del gruppo di regole. Per informazioni su questa opzione, consulta Le azioni sostituiscono i gruppi di regole la Guida per gli AWS WAF sviluppatori.
   - Alcuni gruppi di regole gestiti richiedono una configurazione aggiuntiva. Consulta la documentazione del tuo fornitore di gruppi di regole gestiti. Per informazioni specifiche sui gruppi di regole AWS Managed Rules, AWS Regole gestite per AWS WAF consulta la Guida per gli AWS WAF sviluppatori.

   Quando hai finito con le impostazioni, scegli Salva regola.

10. Impostare l'operazione predefinita per l'ACL Web. Questa è l'azione che AWS WAF intraprende quando una richiesta web non corrisponde a nessuna delle regole dell'ACL web. Puoi aggiungere intestazioni personalizzate con l'azione Consenti o risposte personalizzate per l'azione Blocca. Per ulteriori informazioni sulle azioni ACL Web predefinite, consulta. L'azione predefinita dell'ACL Web Per informazioni sull'impostazione di richieste e risposte Web personalizzate, vedereRichieste e risposte web personalizzate in AWS WAF.
11. Per la configurazione della registrazione, scegli Abilita registrazione per attivare la registrazione. La registrazione fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. Scegli la destinazione di registrazione, quindi scegli la destinazione di registrazione che hai configurato. È necessario scegliere una destinazione di registrazione il cui nome inizi con. `aws-waf-logs-` Per informazioni sulla configurazione di una destinazione di AWS WAF registrazione, vedere. Configurazione della registrazione per una policy AWS WAF
12. (Facoltativo) Se non si desidera che determinati campi e i relativi valori vengano inclusi nei log, omettere tali campi. Scegliere il campo da omettere, quindi selezionare Add (Aggiungi). Se necessario, ripetere l'operazione per omettere i campi aggiuntivi. I campi omessi vengono

visualizzati come `REDACTED` nei log. Ad esempio, se si oscura il campo URI, il campo URI nei registri sarà. `REDACTED`

13. (Facoltativo) Se non desideri inviare tutte le richieste ai log, aggiungi i criteri e il comportamento di filtro. In Filtra log, per ogni filtro che desideri applicare, scegli Aggiungi filtro, quindi scegli i criteri di filtro e specifica se desideri conservare o eliminare le richieste che corrispondono ai criteri. Al termine dell'aggiunta dei filtri, se necessario, modifica il comportamento di registrazione predefinito. Per ulteriori informazioni, consulta la sezione Gestione della registrazione per un ACL Web nella Guida per gli sviluppatori di AWS WAF .
14. È possibile definire un elenco di domini Token per abilitare la condivisione dei token tra applicazioni protette. I token vengono utilizzati dalle Challenge azioni CAPTCHA e e dagli SDK di integrazione delle applicazioni implementati quando si utilizzano i gruppi di regole AWS Managed Rules for AWS WAF Fraud Control, Account Takeover Prevention (ATP) e Bot Control. AWS WAF

    I suffissi pubblici non sono consentiti. Ad esempio, non puoi usare `gov.au` or `co.uk` come dominio token.

    Per impostazione predefinita, AWS WAF accetta token solo per il dominio della risorsa protetta. Se aggiungi domini token in questo elenco, AWS WAF accetta token per tutti i domini dell'elenco e per il dominio della risorsa associata. Per ulteriori informazioni, consulta la sezione Configurazione dell'elenco dei domini del token ACL Web nella Guida per gli sviluppatori di AWS WAF .

    È possibile modificare il CAPTCHA dell'ACL Web e contestare i tempi di immunità solo quando si modifica un ACL Web esistente. È possibile trovare queste impostazioni nella pagina dei dettagli della politica di Firewall Manager. Per informazioni su queste impostazioni, consulta Scadenza del timestamp: tempi di immunità dei token. Se aggiorni le impostazioni Association config, CAPTCHA, Challenge o Token domain list in una policy esistente, Firewall Manager sovrascriverà gli ACL web locali con i nuovi valori. Tuttavia, se non aggiorni le impostazioni dell'elenco di domini Association Config, CAPTCHA, Challenge o Token della policy, i valori negli ACL web locali rimarranno invariati. Per informazioni su questa opzione, consulta la Guida per gli sviluppatoriCAPTCHAe Challenge in AWS WAF.AWS WAF
15. In Gestione ACL Web, se desideri che Firewall Manager gestisca gli ACL Web non associati, abilita Gestisci ACL Web non associati. Con questa opzione, Firewall Manager crea ACL Web negli account inclusi nell'ambito delle policy solo se gli ACL Web verranno utilizzati da almeno una risorsa. Se in qualsiasi momento un account rientra nell'ambito delle politiche, Firewall Manager crea automaticamente un ACL Web nell'account se almeno una risorsa utilizzerà l'ACL

Web. Dopo l'attivazione di questa opzione, Firewall Manager esegue una pulizia una tantum degli ACL Web non associati nell'account. Il processo di pulizia può richiedere diverse ore. Se una risorsa esce dall'ambito delle policy dopo che Firewall Manager ha creato un ACL Web, Firewall Manager dissocia la risorsa dall'ACL Web, ma non ripulisce l'ACL Web non associato. Firewall Manager pulisce gli ACL Web non associati solo quando si abilita per la prima volta la gestione degli ACL Web non associati in una policy.

16. Per l'azione relativa alle politiche, se desideri creare un ACL Web in ogni account applicabile all'interno dell'organizzazione, ma non applicare ancora l'ACL Web a nessuna risorsa, scegli Identifica le risorse che non rispettano le regole delle policy, ma non correggono automaticamente e non scegli Gestisci ACL Web non associati. Puoi modificare queste opzioni in un secondo momento.

    Se invece si desidera applicare automaticamente la policy alle risorse esistenti nell'ambito, scegliere Auto remediate any noncompliant resources (Correggi automaticamente risorse non conformi). Se l'opzione Gestisci ACL Web non associati è disabilitata, l'opzione Riparazione automatica di qualsiasi risorsa non conforme crea un ACL Web in ogni account applicabile all'interno dell'organizzazione e associa l'ACL Web alle risorse degli account. Se l'opzione Gestisci ACL Web non associati è abilitata, l'opzione Riparazione automatica di qualsiasi risorsa non conforme crea e associa un ACL Web solo negli account che dispongono di risorse idonee per l'associazione all'ACL Web.

    Quando scegli Riparazione automatica di qualsiasi risorsa non conforme, puoi anche scegliere di rimuovere le associazioni ACL Web esistenti dalle risorse relative all'ambito, per le ACL Web che non sono gestite da un'altra politica attiva di Firewall Manager. Se si sceglie questa opzione, Firewall Manager associa innanzitutto l'ACL Web della policy alle risorse, quindi rimuove le associazioni precedenti. Se una risorsa ha un'associazione con un altro ACL Web gestito da una politica di Firewall Manager attiva diversa, questa scelta non influisce su tale associazione.

17. Seleziona Successivo.

18. Affinché Account AWS questa politica si applichi a, scegli l'opzione seguente:

    - Se desideri applicare la politica a tutti gli account della tua organizzazione, lascia la selezione predefinita Includi tutti gli account della mia AWS organizzazione.
    - Se desideri applicare la politica solo a conti specifici o account appartenenti a unità AWS Organizations organizzative (OU) specifiche, scegli Includi solo gli account e le unità organizzative specificati, quindi aggiungi gli account e le unità organizzative che desideri includere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità

organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

- Se si desidera applicare la policy a tutti gli account o unità organizzative AWS Organizations tranne uno specifico, scegliere Exclude the specified accounts and organizational units, and include all others (Escludi gli account e le unità organizzative specificati e includi tutti gli altri), quindi aggiungere gli account e le unità organizzative che si desidera escludere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

È possibile scegliere solo una delle opzioni.

Dopo aver applicato la policy, Firewall Manager valuta automaticamente tutti i nuovi account in base alle impostazioni dell'utente. Ad esempio, se includi solo account specifici, Firewall Manager non applica la politica a nessun nuovo account. Come altro esempio, se si include un'unità organizzativa, quando si aggiunge un account all'unità organizzativa o a una delle relative unità organizzative secondarie, Firewall Manager applica automaticamente la politica al nuovo account.

19. Per Resource type (Tipo di risorsa), scegliere i tipi di risorsa che si desidera proteggere.
20. In Resources (Risorse), se si desidera proteggere (o escludere) solo le risorse con tag specifici, selezionare l'opzione appropriata, quindi immettere i tag da includere o escludere. È possibile scegliere una sola opzione. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .

    Se si immettono più tag, una risorsa deve avere tutti i tag da includere o escludere.
21. Seleziona Successivo.
22. Per i tag Policy, aggiungi tutti i tag identificativi che desideri per la policy di Firewall Manager. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .
23. Seleziona Successivo.
24. Rivedere la nuova policy. Per apportare eventuali modifiche, scegliere Edit (Modifica) nell'area che si desidera modificare. In questo modo si torna al passaggio corrispondente della creazione guidata. Al termine, scegliere Create policy (Crea policy).

Creazione di una AWS Firewall Manager politica per AWS WAF Classic

Per creare una policy Firewall Manager per AWS WAF Classic (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Scegli Crea policy.
4. Per Policy type (Tipo di policy), scegliere AWS WAF Classic.
5. Se hai già creato il gruppo di regole AWS WAF Classic che desideri aggiungere alla policy, scegli Crea una AWS Firewall Manager policy e aggiungi gruppi di regole esistenti. Se desideri creare un nuovo gruppo di regole, scegli Crea una politica di Firewall Manager e aggiungi un nuovo gruppo di regole.
6. Per Regione, scegli un Regione AWS. Per proteggere CloudFront le risorse di Amazon, scegli Global.

   Per proteggere le risorse in più regioni (diverse dalle CloudFront risorse), è necessario creare policy Firewall Manager separate per ogni regione.
7. Seleziona Successivo.
8. Se si crea un gruppo di regole, seguire le istruzioni in Creazione di un gruppo di regole AWS WAF classico. Una volta creato il gruppo di regole, procedere nel seguente modo.
9. Inserire un nome per la policy.
10. Se si aggiunge un gruppo di regole esistente, utilizzare il menu a discesa per selezionare un gruppo di regole da aggiungere, quindi scegliere Add rule group (Aggiungi gruppo di regole).
11. È possibile eseguire due operazioni su una policy: Action set by rule group (Operazione impostata dal gruppo di regole) e Count (Contare). Se si desidera verificare la policy e il gruppo di regole, impostare l'operazione su Count (Contare). Questa operazione sostituisce tutte le operazioni di blocco specificate dalle regole nel gruppo di regole. In altre parole, se l'operazione

della policy è impostata su Count (Contare), le relative richieste vengono solo contate, non bloccate. Al contrario, se l'operazione della policy è impostata su Action set by rule group (Operazione impostata dal gruppo di regole), vengono utilizzate le operazioni della regola nel gruppo di regole. Scegliere l'operazione appropriata.

12. Seleziona Successivo.
13. A cui si applica Account AWS questa politica, scegli l'opzione seguente:

    - Se desideri applicare la politica a tutti gli account della tua organizzazione, lascia la selezione predefinita Includi tutti gli account della mia AWS organizzazione.
    - Se desideri applicare la politica solo a conti specifici o account appartenenti a unità AWS Organizations organizzative (OU) specifiche, scegli Includi solo gli account e le unità organizzative specificati, quindi aggiungi gli account e le unità organizzative che desideri includere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.
    - Se desideri applicare la politica a tutti i conti o le unità AWS Organizations organizzative (OU) tranne uno specifico, scegli Escludi gli account e le unità organizzative specificati e includi tutti gli altri, quindi aggiungi gli account e le unità organizzative che desideri escludere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

    È possibile scegliere solo una delle opzioni.

    Dopo aver applicato la policy, Firewall Manager valuta automaticamente tutti i nuovi account in base alle impostazioni dell'utente. Ad esempio, se includi solo account specifici, Firewall Manager non applica la politica a nessun nuovo account. Come altro esempio, se si include un'unità organizzativa, quando si aggiunge un account all'unità organizzativa o a una delle relative unità organizzative secondarie, Firewall Manager applica automaticamente la politica al nuovo account.
14. Scegliere il tipo di risorsa da proteggere.
15. Se si desidera proteggere solo le risorse con tag specifici oppure escludere le risorse con tag specifici, selezionare Use tags to include/exclude resources (Usa tag per includere/escludere risorse), inserire i tag e quindi scegliere Include (Includi) o Exclude (Escludi). È possibile scegliere una sola opzione.

Se inserisci più di un tag (separati da virgole), viene considerata una corrispondenza se una risorsa presenta uno di questi tag.

Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .

16. Se si desidera applicare automaticamente la policy alle risorse esistenti, scegliere Create and apply this policy to existing and new resources (Crea e applica questa policy alle risorse esistenti e nuove).

    Questa opzione crea un'ACL Web in ogni account applicabile all'interno di un'organizzazione in AWS e associa l'ACL Web alle risorse specificate negli account. Inoltre, questa opzione applica la policy a tutte le nuove risorse che soddisfano i criteri precedenti (tipo di risorsa e tag). In alternativa, se si sceglie Create policy but do not apply the policy to existing or new resources (Crea policy ma non applicare la policy a risorse esistenti o nuove), Firewall Manager crea un'ACL Web in ogni account applicabile all'interno dell'organizzazione, ma non applica l'ACL Web ad alcuna risorsa. In seguito sarà necessario applicare la policy alle risorse. Scegliere l'opzione appropriata.

17. Per Replace existing associated web ACLs (Sostituisci gli ACL Web associati esistenti), è possibile scegliere di rimuovere tutte le associazioni di ACL Web attualmente definite per le risorse nell'ambito e quindi sostituirle con associazioni agli ACL Web che si sta creando con questa policy. Per impostazione predefinita, Firewall Manager non rimuove le associazioni ACL Web esistenti prima di aggiungere quelle nuove. Se si desidera rimuovere quelli esistenti, scegliere questa opzione.
18. Seleziona Successivo.
19. Rivedere la nuova policy. Per apportare una modifica, scegliere Edit (Modifica). Al termine, scegliere Create and apply policy (Crea e applica policy).

Creazione di una AWS Firewall Manager politica per AWS Shield Advanced

Per creare una policy Firewall Manager per Shield Advanced (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

> **Note**
>
> Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Scegli Crea policy.
4. Per Tipo di policy, scegli Shield Advanced.

   Per creare una politica Shield Advanced, devi essere abbonato a Shield Advanced. Se non si è iscritti, viene richiesto di farlo. Per informazioni sul costo dell'abbonamento, consulta AWS Shield Advanced la sezione Prezzi.
5. Per Regione, scegli un Regione AWS. Per proteggere le CloudFront distribuzioni Amazon, scegli Global.

   Per le scelte regionali diverse da Global, per proteggere le risorse in più regioni, è necessario creare una politica Firewall Manager separata per ciascuna regione.
6. Seleziona Successivo.
7. Per Nome, inserisci un nome descrittivo.
8. Solo per le politiche della regione globale, puoi scegliere se gestire la mitigazione automatica degli attacchi DDoS a livello di applicazione Shield Advanced. Per informazioni su questa funzionalità Shield Advanced, vedereMitigazione DDoS automatica a livello di applicazione Shield Advanced.

   Puoi scegliere di abilitare o disabilitare la mitigazione automatica oppure puoi scegliere di ignorarla. Se scegli di ignorarlo, Firewall Manager non gestisce affatto la mitigazione automatica per le protezioni Shield Advanced. Per ulteriori informazioni su queste opzioni di policy, consulta. Mitigazione automatica degli attacchi DDoS a livello di applicazione
9. In Gestione ACL Web, se desideri che Firewall Manager gestisca gli ACL Web non associati, abilita Gestisci ACL Web non associati. Con questa opzione, Firewall Manager crea ACL Web negli account inclusi nell'ambito delle policy solo se gli ACL Web verranno utilizzati da almeno una risorsa. Se in qualsiasi momento un account rientra nell'ambito delle politiche, Firewall Manager crea automaticamente un ACL Web nell'account se almeno una risorsa utilizzerà l'ACL Web. Dopo l'attivazione di questa opzione, Firewall Manager esegue una pulizia una tantum degli ACL Web non associati nell'account. Il processo di pulizia può richiedere diverse ore. Se una risorsa esce dall'ambito delle policy dopo che Firewall Manager ha creato un ACL

Web, Firewall Manager non dissocierà la risorsa dall'ACL Web. Per includere l'ACL Web nella pulizia unica, è necessario innanzitutto dissociare manualmente le risorse dall'ACL Web e quindi abilitare Gestisci ACL Web non associati.

10. Per quanto riguarda le azioni relative alle politiche, consigliamo di creare la policy con l'opzione che non corregga automaticamente le risorse non conformi. Quando si disabilita la riparazione automatica, è possibile valutare gli effetti della nuova politica prima di applicarla. Quando ritieni che le modifiche siano quelle che desideri, modifica la politica e modifica l'azione della politica per abilitare la correzione automatica.

    Se invece si desidera applicare automaticamente la policy alle risorse esistenti nell'ambito, scegliere Auto remediate any noncompliant resources (Correggi automaticamente risorse non conformi). Questa opzione applica le protezioni Shield Advanced per ogni account applicabile all'interno AWS dell'organizzazione e ogni risorsa applicabile negli account.

    Solo per le politiche della regione globale, se si sceglie Riparazione automatica di eventuali risorse non conformi, è anche possibile scegliere di fare in modo che Firewall Manager sostituisca automaticamente tutte le associazioni ACL Web AWS WAF classiche esistenti con nuove associazioni agli ACL Web creati utilizzando l'ultima versione di (v2). AWS WAF Se si sceglie questa opzione, Firewall Manager rimuove le associazioni con gli ACL Web della versione precedente e crea nuove associazioni con gli ACL Web della versione più recente, dopo aver creato nuovi ACL Web vuoti in tutti gli account interessati che non li hanno già per la policy. Per ulteriori informazioni su questa opzione, consulta Sostituisci gli ACL web AWS WAF classici con gli ACL web della versione più recente.
11. Seleziona Successivo.
12. A cui si applica Account AWS questa politica, scegli l'opzione seguente:

    - Se desideri applicare la politica a tutti gli account della tua organizzazione, mantieni la selezione predefinita, Includi tutti gli account della mia AWS organizzazione.
    - Se desideri applicare la politica solo a conti specifici o account appartenenti a unità AWS Organizations organizzative (OU) specifiche, scegli Includi solo gli account e le unità organizzative specificati, quindi aggiungi gli account e le unità organizzative che desideri includere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.
    - Se desideri applicare la politica a tutti i conti o le unità AWS Organizations organizzative (OU) tranne uno specifico, scegli Escludi gli account e le unità organizzative specificati e includi tutti

gli altri, quindi aggiungi gli account e le unità organizzative che desideri escludere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

È possibile scegliere solo una delle opzioni.

Dopo aver applicato la policy, Firewall Manager valuta automaticamente tutti i nuovi account in base alle impostazioni dell'utente. Ad esempio, se includi solo account specifici, Firewall Manager non applica la politica a nessun nuovo account. Come altro esempio, se si include un'unità organizzativa, quando si aggiunge un account all'unità organizzativa o a una delle relative unità organizzative secondarie, Firewall Manager applica automaticamente la politica al nuovo account.

13. Scegliere il tipo di risorsa da proteggere.

    Firewall Manager non supporta Amazon Route 53 o AWS Global Accelerator. Se è necessario utilizzare Shield Advanced per proteggere le risorse da questi servizi, non è possibile utilizzare una policy Firewall Manager. Segui invece la guida Shield Advanced all'indirizzoAggiungere AWS Shield Advanced protezione alle risorse AWS.

14. Se desideri proteggere solo risorse con tag specifici o, in alternativa, escludere risorse con tag specifici, seleziona Usa tag per includere/escludere risorse, inserisci i tag separati da virgole, quindi scegli Includi o Escludi. È possibile scegliere una sola opzione.

    Se inserisci più di un tag e se una risorsa ha uno di questi tag, viene considerata una corrispondenza.

    Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .

15. Seleziona Successivo.

16. Per i tag Policy, aggiungi tutti i tag identificativi che desideri per la policy di Firewall Manager. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .

17. Seleziona Successivo.

18. Rivedere la nuova policy. Per apportare eventuali modifiche, scegliere Edit (Modifica) nell'area che si desidera modificare. In questo modo si torna al passaggio corrispondente della creazione guidata. Al termine, scegliere Create policy (Crea policy).

Creazione di una policy di gruppo di sicurezza comune AWS Firewall Manager

Per informazioni sul funzionamento dei criteri comuni dei gruppi di protezione, vedere Policy di gruppo di sicurezza comuni.

Per creare una politica di gruppo di sicurezza comune, è necessario disporre di un gruppo di sicurezza già creato nell'account amministratore di Firewall Manager che si desidera utilizzare come principale per la politica. Puoi gestire i gruppi di sicurezza tramite Amazon Virtual Private Cloud (Amazon VPC) o Amazon Elastic Compute Cloud (Amazon EC2) Elastic Compute Cloud (Amazon EC2). Per informazioni, consulta Working with Security Groups nella Amazon VPC User Guide.

Per creare un criterio di gruppo di protezione comune (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Scegli Crea policy.
4. Per Tipo di criterio, scegliere Gruppo di protezione.
5. Per Tipo di criteri di gruppo di protezione, scegliere Gruppi di protezione comuni.
6. Per Regione, scegli un Regione AWS.
7. Seleziona Successivo.
8. Per Nome criterio, immettere un nome descrittivo.
9. Per Regole criteri, eseguire le operazioni seguenti:

   a. Dall'opzione regole, scegli le restrizioni che desideri applicare alle regole del gruppo di sicurezza e alle risorse che rientrano nell'ambito della politica. Se scegli Distribuisci i tag dal gruppo di sicurezza principale ai gruppi di sicurezza creati da questa politica, devi anche selezionare Identifica e segnala quando i gruppi di sicurezza creati da questa politica diventano non conformi.

> **Important**
>
> Firewall Manager non distribuirà i tag di sistema aggiunti dai AWS servizi nei gruppi di sicurezza delle repliche. I tag di sistema iniziano con il prefisso `aws:`. Inoltre, Firewall Manager non aggiornerà i tag dei gruppi di sicurezza esistenti né creerà nuovi gruppi di sicurezza se la policy contiene tag che sono in conflitto con la politica dei tag dell'organizzazione. Per informazioni sulle politiche relative ai tag, consulta le politiche relative ai tag nella Guida AWS Organizations per l'utente.

Se scegli Distribuisci i riferimenti ai gruppi di sicurezza dal gruppo di sicurezza principale ai gruppi di sicurezza creati da questa politica, Firewall Manager distribuisce i riferimenti ai gruppi di sicurezza solo se dispongono di una connessione peering attiva in Amazon VPC. Per informazioni su questa opzione, consulta le impostazioni delle regole di policy.

b. Per i gruppi di sicurezza primari, scegli Aggiungi gruppo di sicurezza primario, quindi scegli il gruppo di sicurezza che desideri utilizzare. Firewall Manager compila l'elenco dei gruppi di sicurezza primari di tutte le istanze Amazon VPC nell'account amministratore di Firewall Manager. Il numero massimo per i gruppi di sicurezza primari per una policy è uno. Per informazioni su come aumentare il numero massimo, consultare AWS Firewall Manager quote.

c. Per azione criteri, si consiglia di creare il criterio con l'opzione che non risolve automaticamente. In questo modo è possibile valutare gli effetti della nuova politica prima di applicarla. Quando si è certi che le modifiche sono ciò che si desidera, modificare il criterio e modificare l'azione del criterio per abilitare la correzione automatica delle risorse non conformi.

10. Seleziona Successivo.
11. A cui si applica Account AWS questa politica, scegli l'opzione seguente:

    - Se desideri applicare la politica a tutti gli account della tua organizzazione, lascia la selezione predefinita Includi tutti gli account della mia AWS organizzazione.
    - Se desideri applicare la politica solo a conti specifici o account appartenenti a unità AWS Organizations organizzative (OU) specifiche, scegli Includi solo gli account e le unità organizzative specificati, quindi aggiungi gli account e le unità organizzative che desideri includere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità

organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

- Se desideri applicare la politica a tutti i conti o le unità AWS Organizations organizzative (OU) tranne uno specifico, scegli Escludi gli account e le unità organizzative specificati e includi tutti gli altri, quindi aggiungi gli account e le unità organizzative che desideri escludere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

È possibile scegliere solo una delle opzioni.

Dopo aver applicato la policy, Firewall Manager valuta automaticamente tutti i nuovi account in base alle impostazioni dell'utente. Ad esempio, se includi solo account specifici, Firewall Manager non applica la politica a nessun nuovo account. Come altro esempio, se si include un'unità organizzativa, quando si aggiunge un account all'unità organizzativa o a una delle relative unità organizzative secondarie, Firewall Manager applica automaticamente la politica al nuovo account.

12. Per Resource type (Tipo di risorsa), scegliere i tipi di risorsa che si desidera proteggere.

    Se scegli un'istanza EC2, puoi scegliere di includere tutte le interfacce di rete elastiche in ogni istanza Amazon EC2 o solo l'interfaccia predefinita in ogni istanza. Se disponi di più di un'interfaccia di rete elastica in qualsiasi istanza Amazon EC2 pertinente, la scelta dell'opzione per includere tutte le interfacce consente a Firewall Manager di applicare la policy a tutte. Quando abiliti la riparazione automatica, se Firewall Manager non è in grado di applicare la policy a tutte le interfacce di rete elastiche in un'istanza Amazon EC2, contrassegna l'istanza come non conforme.

13. Per Risorse, se desideri applicare la policy a tutte le risorse all'interno dei parametri Account AWS e del tipo di risorsa, scegli Includi tutte le risorse che corrispondono al tipo di risorsa selezionato. Se si desidera includere o escludere risorse specifiche, utilizzare il tag per specificare le risorse, quindi scegliere l'opzione appropriata e aggiungere i tag all'elenco. È possibile applicare il criterio a tutte le risorse ad eccezione di quelle che dispongono di tutti i tag specificati oppure è possibile applicarlo solo a quelle che dispongono di tutti i tag specificati. Per ulteriori informazioni sull'assegnazione di tag alle risorse, vedere Utilizzo dell'editor dei tag.

> **Note**
>
> Se si immettono più tag, una risorsa deve avere tutti i tag per essere una corrispondenza.

14. Per Shared VPC resources (Risorse VPC condivisi), se si desidera applicare la policy alle risorse in VPC condivisi, oltre ai VPC proprietari degli account, selezionare Include resources from shared VPCs (Includi risorse da VPC condivisi).
15. Seleziona Successivo.
16. Esaminare le impostazioni dei criteri per accertarsi che siano ciò che si desidera, quindi scegliere Crea criterio.

Firewall Manager crea una replica del gruppo di sicurezza primario in ogni istanza Amazon VPC contenuta negli account interessati fino alla quota massima supportata di Amazon VPC per account. Firewall Manager associa i gruppi di sicurezza delle repliche alle risorse che rientrano nell'ambito delle policy per ogni account compreso nell'ambito. Per ulteriori informazioni su come effettuare tale operazione, consulta Policy di gruppo di sicurezza comuni.

Creazione di una policy di gruppo di sicurezza di controllo del contenuto AWS Firewall Manager

Per informazioni sul funzionamento dei criteri dei gruppi di protezione del controllo del contenuto, vedere Policy di gruppo di sicurezza del controllo dei contenuti.

Per alcune impostazioni dei criteri di controllo dei contenuti, è necessario fornire un gruppo di sicurezza di controllo per Firewall Manager da utilizzare come modello. Ad esempio, potresti avere un gruppo di sicurezza di controllo che contenga tutte le regole che non consentite in nessun gruppo di sicurezza. È necessario creare questi gruppi di sicurezza di controllo utilizzando l'account amministratore di Firewall Manager, prima di poterli utilizzare nella politica. Puoi gestire i gruppi di sicurezza tramite Amazon Virtual Private Cloud (Amazon VPC) o Amazon Elastic Compute Cloud (Amazon EC2) Elastic Compute Cloud (Amazon EC2). Per informazioni, consulta Working with Security Groups nella Amazon VPC User Guide.

Per creare un criterio di gruppo di protezione del controllo del contenuto (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/

fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

> **Note**
>
> Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Scegli Crea policy.
4. Per Tipo di criterio, scegliere Gruppo di protezione.
5. Per Tipo di criteri di gruppo di protezione, scegliere Controllo e applicazione delle regole dei gruppi di protezione.
6. Per Regione, scegli un Regione AWS.
7. Seleziona Successivo.
8. Per Nome criterio, immettere un nome descrittivo.
9. Per le regole delle politiche, scegli l'opzione relativa alle regole politiche gestite o personalizzate che desideri utilizzare.

    a. Per Configura le regole delle politiche di controllo gestite, procedi come segue:

        i. In Configura le regole del gruppo di sicurezza da controllare, seleziona il tipo di regole del gruppo di sicurezza a cui desideri applicare la politica di controllo.

        ii. Se desideri eseguire operazioni come regole di controllo basate sui protocolli, sulle porte e sulle impostazioni dell'intervallo CIDR presenti nei tuoi gruppi di sicurezza, scegli Controlla le regole del gruppo di sicurezza eccessivamente permissive e seleziona le opzioni che desideri.

            Per la selezione La regola consente tutto il traffico, puoi fornire un elenco di applicazioni personalizzato per designare le applicazioni che desideri controllare. Per informazioni sugli elenchi di applicazioni personalizzati e su come utilizzarli nella politica, consulta Elenchi gestiti eUtilizzo di elenchi gestiti.

            Per le selezioni che utilizzano elenchi di protocolli, è possibile utilizzare elenchi esistenti e creare nuovi elenchi. Per informazioni sugli elenchi di protocolli e su come utilizzarli nella politica, vedere Elenchi gestiti eUtilizzo di elenchi gestiti.

iii. Se desideri controllare le applicazioni ad alto rischio in base al loro accesso a intervalli CIDR riservati o non riservati, scegli Controlla le applicazioni ad alto rischio e seleziona le opzioni desiderate.

Le seguenti selezioni si escludono a vicenda: Applicazioni che possono accedere solo a intervalli CIDR riservati e Applicazioni autorizzate ad accedere a intervalli CIDR non riservati. È possibile selezionarne al massimo uno in qualsiasi politica.

Per le selezioni che utilizzano elenchi di applicazioni, è possibile utilizzare elenchi esistenti e creare nuovi elenchi. Per informazioni sugli elenchi di applicazioni e su come utilizzarli nella politica, vedere Elenchi gestiti eUtilizzo di elenchi gestiti.

iv. Utilizza le impostazioni Overrides per sovrascrivere in modo esplicito le altre impostazioni della politica. Puoi scegliere di consentire o negare sempre regole specifiche del gruppo di sicurezza, indipendentemente dal fatto che siano conformi alle altre opzioni che hai impostato per la policy.

Per questa opzione, fornisci un gruppo di sicurezza di controllo come modello di regole consentite o negate. Per i gruppi di sicurezza di controllo, scegli Aggiungi gruppi di sicurezza di controllo, quindi scegli il gruppo di sicurezza che desideri utilizzare. Firewall Manager compila l'elenco dei gruppi di sicurezza di controllo di tutte le istanze Amazon VPC nell'account amministratore di Firewall Manager. La quota massima predefinita per il numero di gruppi di sicurezza di controllo per una policy è uno. Per informazioni su come aumentare la quota, consultare AWS Firewall Manager quote.

b. Per Configurare le regole delle policy personalizzate, procedi come segue:

i. Dalle opzioni regole scegliere se consentire solo le regole definite nei gruppi di sicurezza di controllo o negare tutte le regole. Per informazioni su questa scelta, vedere Policy di gruppo di sicurezza del controllo dei contenuti.

ii. Per i gruppi di sicurezza di controllo, scegli Aggiungi gruppi di sicurezza di controllo, quindi scegli il gruppo di sicurezza che desideri utilizzare. Firewall Manager compila l'elenco dei gruppi di sicurezza di controllo di tutte le istanze Amazon VPC nell'account amministratore di Firewall Manager. La quota massima predefinita per il numero di gruppi di sicurezza di controllo per una policy è uno. Per informazioni su come aumentare la quota, consultare AWS Firewall Manager quote.

iii. Per azione criteri, è necessario creare il criterio con l'opzione che non si aggiorna automaticamente. In questo modo è possibile valutare gli effetti della nuova politica prima di applicarla. Quando si è certi che le modifiche sono ciò che si desidera,

modificare il criterio e modificare l'azione del criterio per abilitare la correzione automatica delle risorse non conformi.

10. Seleziona Successivo.
11. A cui si applica Account AWS questa politica, scegli l'opzione seguente:

    - Se desideri applicare la politica a tutti gli account della tua organizzazione, lascia la selezione predefinita Includi tutti gli account della mia AWS organizzazione.
    - Se desideri applicare la politica solo a conti specifici o account appartenenti a unità AWS Organizations organizzative (OU) specifiche, scegli Includi solo gli account e le unità organizzative specificati, quindi aggiungi gli account e le unità organizzative che desideri includere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.
    - Se desideri applicare la politica a tutti i conti o le unità AWS Organizations organizzative (OU) tranne uno specifico, scegli Escludi gli account e le unità organizzative specificati e includi tutti gli altri, quindi aggiungi gli account e le unità organizzative che desideri escludere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

    È possibile scegliere solo una delle opzioni.

    Dopo aver applicato la policy, Firewall Manager valuta automaticamente tutti i nuovi account in base alle impostazioni dell'utente. Ad esempio, se includi solo account specifici, Firewall Manager non applica la politica a nessun nuovo account. Come altro esempio, se si include un'unità organizzativa, quando si aggiunge un account all'unità organizzativa o a una delle relative unità organizzative secondarie, Firewall Manager applica automaticamente la politica al nuovo account.
12. Per Tipo di risorsa, scegliere i tipi di risorsa che si desidera proteggere.
13. Per Risorse, se desideri applicare la politica a tutte le risorse all'interno dei parametri Account AWS e del tipo di risorsa, scegli Includi tutte le risorse che corrispondono al tipo di risorsa selezionato. Se si desidera includere o escludere risorse specifiche, utilizzare il tag per specificare le risorse, quindi scegliere l'opzione appropriata e aggiungere i tag all'elenco. È possibile applicare il criterio a tutte le risorse ad eccezione di quelle che dispongono di tutti i tag specificati oppure è possibile applicarlo solo a quelle che dispongono di tutti i tag specificati. Per ulteriori informazioni sull'assegnazione di tag alle risorse, vedere Utilizzo dell'editor dei tag.

> **Note**
>
> Se si immettono più tag, una risorsa deve avere tutti i tag per essere una corrispondenza.

14. Seleziona Successivo.
15. Esaminare le impostazioni dei criteri per accertarsi che siano ciò che si desidera, quindi scegliere Crea criterio.

Firewall Manager confronta il gruppo di sicurezza di controllo con i gruppi di sicurezza pertinenti all'interno AWS dell'organizzazione, in base alle impostazioni delle regole dei criteri. È possibile verificare lo stato delle politiche nella console delle AWS Firewall Manager politiche. Dopo aver creato il criterio, è possibile modificarlo e abilitare la correzione automatica per rendere effettivi i criteri del gruppo di protezione del controllo. Per ulteriori informazioni su come effettuare tale operazione, consulta Policy di gruppo di sicurezza del controllo dei contenuti.

Creazione di una policy di gruppo di sicurezza di controllo dell'utilizzo AWS Firewall Manager

Per informazioni sul funzionamento dei criteri dei gruppi di protezione del controllo dell'utilizzo, vedere Policy di gruppo di sicurezza controllo dell'utilizzo.

Per creare un criterio di gruppo di protezione controllo dell'utilizzo (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Scegli Crea policy.
4. Per Tipo di criterio, scegliere Gruppo di protezione.

5. Per il tipo di policy del gruppo di sicurezza, scegli Controllo e pulizia dei gruppi di sicurezza non associati e ridondanti.
6. Per Regione, scegli un. Regione AWS
7. Seleziona Successivo.
8. Per Nome criterio, immettere un nome descrittivo.
9. Per Regole dei criteri, scegliere una o entrambe le opzioni disponibili.

   - Se si sceglie che i gruppi di sicurezza all'interno di questo ambito di policy devono essere utilizzati da almeno una risorsa, Firewall Manager rimuove tutti i gruppi di sicurezza che ritiene non utilizzati. Quando questa regola è abilitata, Firewall Manager la esegue per ultimo quando si salva la policy.

     Per informazioni dettagliate su come Firewall Manager determina l'utilizzo e la tempistica della riparazione, vedere. Policy di gruppo di sicurezza controllo dell'utilizzo

     > **Note**
     >
     > Quando utilizzate questo tipo di policy del gruppo di sicurezza per il controllo dell'utilizzo, evitate di apportare più modifiche allo stato di associazione dei gruppi di sicurezza interessati in un breve lasso di tempo. In questo modo, Firewall Manager potrebbe perdere gli eventi corrispondenti.

     Per impostazione predefinita, Firewall Manager considera i gruppi di sicurezza non conformi a questa regola politica non appena non vengono utilizzati. Facoltativamente, è possibile specificare il numero di minuti in cui un gruppo di sicurezza può rimanere inutilizzato prima che venga considerato non conforme, fino a 525.600 minuti (365 giorni). Puoi utilizzare questa impostazione per concederti il tempo necessario per associare nuovi gruppi di sicurezza alle risorse.

     > **Important**
     >
     > Se si specifica un numero di minuti diverso dal valore predefinito zero, è necessario abilitare le relazioni indirette in AWS Config. In caso contrario, le politiche del gruppo di sicurezza per il controllo dell'utilizzo non funzioneranno come previsto. Per

informazioni sulle relazioni indirette in AWS Config, vedere Relazioni indirette AWS Config nella Guida per gli AWS Config sviluppatori.

- Se si sceglie che i gruppi di sicurezza all'interno di questo ambito di policy devono essere univoci, Firewall Manager consolida i gruppi di sicurezza ridondanti, in modo che solo uno sia associato a qualsiasi risorsa. Se si sceglie questa opzione, Firewall Manager la esegue per primo quando si salva la policy.

10. Per azione criteri, si consiglia di creare il criterio con l'opzione che non risolve automaticamente. In questo modo è possibile valutare gli effetti della nuova politica prima di applicarla. Quando si è certi che le modifiche sono ciò che si desidera, modificare il criterio e modificare l'azione del criterio per abilitare la correzione automatica delle risorse non conformi.
11. Seleziona Successivo.
12. A cui si applica Account AWS questa politica, scegli l'opzione seguente:

    - Se desideri applicare la politica a tutti gli account della tua organizzazione, lascia la selezione predefinita Includi tutti gli account della mia AWS organizzazione.
    - Se desideri applicare la politica solo a conti specifici o account appartenenti a unità AWS Organizations organizzative (OU) specifiche, scegli Includi solo gli account e le unità organizzative specificati, quindi aggiungi gli account e le unità organizzative che desideri includere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.
    - Se desideri applicare la politica a tutti i conti o le unità AWS Organizations organizzative (OU) tranne uno specifico, scegli Escludi gli account e le unità organizzative specificati e includi tutti gli altri, quindi aggiungi gli account e le unità organizzative che desideri escludere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

    È possibile scegliere solo una delle opzioni.

    Dopo aver applicato la policy, Firewall Manager valuta automaticamente tutti i nuovi account in base alle impostazioni dell'utente. Ad esempio, se includi solo account specifici, Firewall Manager non applica la politica a nessun nuovo account. Come altro esempio, se si include un'unità organizzativa, quando si aggiunge un account all'unità organizzativa o a una delle

relative unità organizzative secondarie, Firewall Manager applica automaticamente la politica al nuovo account.

13. Per Risorse, se desideri applicare la politica a tutte le risorse all'interno dei parametri Account AWS e del tipo di risorsa, scegli Includi tutte le risorse che corrispondono al tipo di risorsa selezionato. Se si desidera includere o escludere risorse specifiche, utilizzare il tag per specificare le risorse, quindi scegliere l'opzione appropriata e aggiungere i tag all'elenco. È possibile applicare il criterio a tutte le risorse ad eccezione di quelle che dispongono di tutti i tag specificati oppure è possibile applicarlo solo a quelle che dispongono di tutti i tag specificati. Per ulteriori informazioni sull'assegnazione di tag alle risorse, vedere Utilizzo dell'editor dei tag.

    > **Note**
    >
    > Se si immettono più tag, una risorsa deve avere tutti i tag per essere una corrispondenza.

14. Seleziona Successivo.
15. Se non è stato escluso l'account amministratore di Firewall Manager dall'ambito delle politiche, Firewall Manager richiede di eseguire questa operazione. In questo modo, i gruppi di sicurezza nell'account amministratore di Firewall Manager, utilizzato per le politiche comuni e di controllo dei gruppi di sicurezza, sono sotto il controllo manuale. Scegli l'opzione desiderata in questa finestra di dialogo.
16. Esaminare le impostazioni dei criteri per accertarsi che siano ciò che si desidera, quindi scegliere Crea criterio.

Se hai scelto di richiedere gruppi di sicurezza unici, Firewall Manager esegue la scansione alla ricerca di gruppi di sicurezza ridondanti in ogni istanza Amazon VPC pertinente. Quindi, se si sceglie di richiedere che ogni gruppo di sicurezza venga utilizzato da almeno una risorsa, Firewall Manager esegue la scansione dei gruppi di sicurezza che sono rimasti inutilizzati per i minuti specificati nella regola. È possibile verificare lo stato della policy nella console delle AWS Firewall Manager policy. Per ulteriori informazioni su come effettuare tale operazione, consulta Policy di gruppo di sicurezza controllo dell'utilizzo.

Creazione di una AWS Firewall Manager politica per AWS Network Firewall

In una politica Firewall Network Firewall di Firewall Manager, si utilizzano i gruppi di regole in cui è possibile gestire AWS Network Firewall. Per informazioni sulla gestione dei gruppi di regole, consulta i gruppi di AWS Network Firewall regole nella Network Firewall Developer Guide.

Per informazioni sulle politiche del firewall di rete di Firewall Manager, vedereAWS Network Firewall politiche.

Per creare una policy Firewall Manager per AWS Network Firewall (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Scegli Crea policy.
4. Per Policy type (Tipo di policy), scegliere AWS Network Firewall.
5. In Tipo di gestione del firewall, scegli come desideri che Firewall Manager gestisca i firewall della policy. Seleziona una delle opzioni seguenti:

   - Distribuito: Firewall Manager crea e gestisce gli endpoint firewall in ogni VPC che rientra nell'ambito della policy.
   - Centralizzato: Firewall Manager crea e gestisce gli endpoint in un unico VPC di ispezione.
   - Importa firewall esistenti - Firewall Manager importa i firewall esistenti da Network Firewall utilizzando set di risorse. Per informazioni sui set di risorse, vedere. Utilizzo dei set di risorse in Firewall Manager

6. Per Regione, scegli un Regione AWS. Per proteggere le risorse in più regioni, devi creare politiche separate per ogni regione.
7. Seleziona Successivo.
8. Per Nome della politica, inserisci un nome descrittivo. Firewall Manager include il nome della policy nei nomi dei firewall Network Firewall e nelle policy firewall che crea.
9. Nella configurazione della AWS Network Firewall politica, configura la politica del firewall come faresti in Network Firewall. Aggiungi i tuoi gruppi di regole stateless e stateful e specifica le azioni predefinite della policy. Facoltativamente, puoi impostare l'ordine di valutazione delle regole stateful e le azioni predefinite della policy, nonché la configurazione della registrazione. Per

informazioni sulla gestione delle policy firewall di Network Firewall, consulta le policy del AWS Network Firewall firewall nella AWS Network Firewall Developer Guide.

Quando si crea la politica Firewall Manager Network Firewall, Firewall Manager crea politiche firewall per gli account che rientrano nell'ambito. I singoli account manager possono aggiungere gruppi di regole alle politiche del firewall, ma non possono modificare la configurazione fornita qui.

10. Seleziona Successivo.
11. Effettua una delle seguenti operazioni, a seconda del tipo di gestione del firewall selezionato nel passaggio precedente:

    - Se utilizzi un tipo di gestione del firewall distribuito, nella configurazione dell'AWS Firewall Manager endpoint in Posizione dell'endpoint Firewall, scegli una delle seguenti opzioni:
      - Configurazione personalizzata degli endpoint: Firewall Manager crea firewall per ogni VPC nell'ambito della policy, nelle zone di disponibilità specificate. Ogni firewall contiene almeno un endpoint firewall.
        - In Zone di disponibilità, seleziona le zone di disponibilità in cui creare gli endpoint del firewall. È possibile selezionare le zone di disponibilità in base al nome della zona di disponibilità o all'ID della zona di disponibilità.
        - Se desideri fornire i blocchi CIDR a Firewall Manager da utilizzare per le sottoreti firewall nei tuoi VPC, devono essere tutti blocchi CIDR /28. Inserisci un blocco per riga. Se li ometti, Firewall Manager sceglie gli indirizzi IP per te tra quelli disponibili nei VPC.

        > **Note**
        >
        > La riparazione automatica viene eseguita automaticamente per le politiche del AWS Firewall Manager Network Firewall, quindi qui non è disponibile un'opzione per scegliere di non eseguire la riparazione automatica.

      - Configurazione automatica degli endpoint: Firewall Manager crea automaticamente endpoint firewall nelle zone di disponibilità con sottoreti pubbliche nel tuo VPC.
        - Per la configurazione degli endpoint del firewall, specificare come si desidera che gli endpoint del firewall vengano gestiti da Firewall Manager. Si consiglia di utilizzare più endpoint per un'elevata disponibilità.

- Se utilizzi un tipo di gestione del firewall centralizzato, nella configurazione degli AWS Firewall Manager endpoint in configurazione Inspection VPC, inserisci l'ID AWS account del proprietario del VPC di ispezione e l'ID VPC del VPC di ispezione.
  - In Zone di disponibilità, seleziona le zone di disponibilità in cui creare gli endpoint del firewall. È possibile selezionare le zone di disponibilità in base al nome della zona di disponibilità o all'ID della zona di disponibilità.
  - Se desideri fornire i blocchi CIDR a Firewall Manager da utilizzare per le sottoreti firewall nei tuoi VPC, devono essere tutti blocchi CIDR /28. Inserisci un blocco per riga. Se li ometti, Firewall Manager sceglie gli indirizzi IP per te tra quelli disponibili nei VPC.

    > **Note**
    >
    > La riparazione automatica viene eseguita automaticamente per le politiche del AWS Firewall Manager Network Firewall, quindi qui non è disponibile un'opzione per scegliere di non eseguire la riparazione automatica.

- Se utilizzi un tipo di gestione del firewall per l'importazione di firewall esistenti, in Set di risorse aggiungi uno o più set di risorse. Un set di risorse definisce i firewall Network Firewall esistenti di proprietà dell'account dell'organizzazione che desideri gestire centralmente in questa politica. Per aggiungere un set di risorse alla policy, devi prima creare un set di risorse utilizzando la console o l'PutResourceSetAPI. Per informazioni sui set di risorse, vedereUtilizzo dei set di risorse in Firewall Manager. Per ulteriori informazioni sull'importazione di firewall esistenti da Network Firewall, vedere importare firewall esistenti.

12. Seleziona Successivo.
13. Se la tua politica utilizza un tipo di gestione del firewall distribuito, in Gestione del percorso, scegli se Firewall Manager monitorerà e avviserà il traffico che deve essere instradato attraverso i rispettivi endpoint del firewall.

    > **Note**
    >
    > Se scegli Monitor, non puoi modificare l'impostazione su Off in un secondo momento. Il monitoraggio continua finché non elimini la politica.

14. Per Tipo di traffico, aggiungi facoltativamente gli endpoint di traffico attraverso i quali desideri indirizzare il traffico per l'ispezione del firewall.

15. Per Consenti il traffico Cross-AZ richiesto, se si abilita questa opzione, Firewall Manager considera un routing conforme che invia il traffico fuori da una zona di disponibilità per l'ispezione, per le zone di disponibilità che non dispongono di un proprio endpoint firewall. Le zone di disponibilità con endpoint devono sempre ispezionare il proprio traffico.
16. Seleziona Successivo.
17. Per l'ambito della policy, ai sensi di Account AWS questa policy, scegliete l'opzione seguente:

    - Se desideri applicare la politica a tutti gli account della tua organizzazione, lascia la selezione predefinita Includi tutti gli account della mia AWS organizzazione.
    - Se desideri applicare la politica solo a conti specifici o account appartenenti a unità AWS Organizations organizzative (OU) specifiche, scegli Includi solo gli account e le unità organizzative specificati, quindi aggiungi gli account e le unità organizzative che desideri includere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.
    - Se desideri applicare la politica a tutti i conti o le unità AWS Organizations organizzative (OU) tranne uno specifico, scegli Escludi gli account e le unità organizzative specificati e includi tutti gli altri, quindi aggiungi gli account e le unità organizzative che desideri escludere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

    È possibile scegliere solo una delle opzioni.

    Dopo aver applicato la policy, Firewall Manager valuta automaticamente tutti i nuovi account in base alle impostazioni dell'utente. Ad esempio, se includi solo account specifici, Firewall Manager non applica la politica a nessun nuovo account. Come altro esempio, se si include un'unità organizzativa, quando si aggiunge un account all'unità organizzativa o a una delle relative unità organizzative secondarie, Firewall Manager applica automaticamente la politica al nuovo account.
18. Il tipo di risorsa per le politiche del Network Firewall è VPC.
19. In Resources (Risorse), se si desidera proteggere (o escludere) solo le risorse con tag specifici, selezionare l'opzione appropriata, quindi immettere i tag da includere o escludere. È possibile scegliere una sola opzione. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .

Se si immettono più tag, una risorsa deve avere tutti i tag da includere o escludere.

20. Seleziona Successivo.
21. Per i tag Policy, aggiungi tutti i tag identificativi che desideri per la policy di Firewall Manager. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .
22. Seleziona Successivo.
23. Rivedere la nuova policy. Per apportare eventuali modifiche, scegliere Edit (Modifica) nell'area che si desidera modificare. In questo modo si torna al passaggio corrispondente della creazione guidata. Al termine, scegliere Create policy (Crea policy).

Creazione di una AWS Firewall Manager policy per Amazon Route 53 Resolver DNS Firewall

In una policy Firewall DNS Firewall Manager, usi i gruppi di regole che gestisci in Amazon Route 53 Resolver DNS Firewall. Per informazioni sulla gestione dei gruppi di regole, consulta Managing rule groups and rules in DNS Firewall nella Amazon Route 53 Developer Guide.

Per informazioni sulle politiche del firewall DNS di Firewall Manager, vederePolitiche del firewall DNS di Amazon Route 53 Resolver.

Per creare una policy Firewall Manager per Amazon Route 53 Resolver DNS Firewall (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Scegli Crea policy.
4. Per Tipo di policy, scegli Amazon Route 53 Resolver DNS Firewall.
5. Per Regione, scegli un Regione AWS. Per proteggere le risorse in più regioni, devi creare politiche separate per ogni regione.

6. Seleziona Successivo.
7. Per Nome della politica, inserisci un nome descrittivo.
8. Nella configurazione delle policy, aggiungi i gruppi di regole che desideri che DNS Firewall valuti per primi e ultimi tra le associazioni dei gruppi di regole dei tuoi VPC. Puoi aggiungere fino a due gruppi di regole alla policy.

   Quando crei la policy Firewall DNS di Firewall Manager, Firewall Manager crea le associazioni dei gruppi di regole, con le priorità di associazione che hai fornito, per i VPC e gli account che rientrano nell'ambito. I singoli account manager possono aggiungere associazioni di gruppi di regole tra la prima e l'ultima associazione, ma non possono modificare le associazioni qui definite. Per ulteriori informazioni, consulta la pagina Politiche del firewall DNS di Amazon Route 53 Resolver.
9. Seleziona Next (Successivo).
10. A cui si applica Account AWS questa politica, scegli l'opzione seguente:

    - Se desideri applicare la politica a tutti gli account della tua organizzazione, lascia la selezione predefinita Includi tutti gli account della mia AWS organizzazione.
    - Se desideri applicare la politica solo a conti specifici o account appartenenti a unità AWS Organizations organizzative (OU) specifiche, scegli Includi solo gli account e le unità organizzative specificati, quindi aggiungi gli account e le unità organizzative che desideri includere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.
    - Se desideri applicare la politica a tutti i conti o le unità AWS Organizations organizzative (OU) tranne uno specifico, scegli Escludi gli account e le unità organizzative specificati e includi tutti gli altri, quindi aggiungi gli account e le unità organizzative che desideri escludere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

    È possibile scegliere solo una delle opzioni.

    Dopo aver applicato la policy, Firewall Manager valuta automaticamente tutti i nuovi account in base alle impostazioni dell'utente. Ad esempio, se includi solo account specifici, Firewall Manager non applica la politica a nessun nuovo account. Come altro esempio, se si include un'unità organizzativa, quando si aggiunge un account all'unità organizzativa o a una delle

relative unità organizzative secondarie, Firewall Manager applica automaticamente la politica al nuovo account.

11. Il tipo di risorsa per le politiche del firewall DNS è VPC.
12. In Resources (Risorse), se si desidera proteggere (o escludere) solo le risorse con tag specifici, selezionare l'opzione appropriata, quindi immettere i tag da includere o escludere. È possibile scegliere una sola opzione. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .

    Se si immettono più tag, una risorsa deve avere tutti i tag da includere o escludere.
13. Seleziona Successivo.
14. Per i tag Policy, aggiungi tutti i tag identificativi che desideri per la policy di Firewall Manager. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .
15. Seleziona Successivo.
16. Rivedere la nuova policy. Per apportare eventuali modifiche, scegliere Edit (Modifica) nell'area che si desidera modificare. In questo modo si torna al passaggio corrispondente della creazione guidata. Al termine, scegliere Create policy (Crea policy).

Creazione di una AWS Firewall Manager policy per Palo Alto Networks Cloud NGFW

Con una policy Firewall Manager per Palo Alto Networks Cloud Next Generation Firewall (Palo Alto Networks Cloud NGFW), utilizzi Firewall Manager per distribuire le risorse Palo Alto Networks Cloud NGFW e gestire gli stack di regole NGFW centralmente su tutti i tuoi account. AWS

Per informazioni sulle politiche NGFW di Firewall Manager Palo Alto Networks Cloud, vedere. Politiche NGFW di Palo Alto Networks Cloud Per informazioni su come configurare e gestire Palo Alto Networks Cloud NGFW for Firewall Manager, vedere Palo Alto Networks Palo Alto Networks Cloud NGFW sulla documentazione. AWS

Prerequisiti

Vi sono diversi passaggi obbligatori per preparare l'account AWS Firewall Manager. Tali fasi sono descritte nell'articolo AWS Firewall Manager prerequisiti. Completa tutti i prerequisiti prima di procedere al passaggio successivo.

Per creare una policy Firewall Manager per Palo Alto Networks Cloud NGFW (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/

fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

> **Note**
>
> Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Scegli Crea policy.
4. Per il tipo di policy, scegli Palo Alto Networks Cloud NGFW. Se non ti sei ancora abbonato al servizio Palo Alto Networks Cloud NGFW nel AWS Marketplace, devi prima farlo. Per iscriverti al AWS Marketplace, scegli Visualizza i dettagli del AWS Marketplace.
5. Per il modello di implementazione, scegli il modello distribuito o il modello centralizzato. Il modello di distribuzione determina il modo in cui Firewall Manager gestisce gli endpoint per la policy. Con il modello distribuito, Firewall Manager mantiene gli endpoint del firewall in ogni VPC che rientra nell'ambito delle policy. Con il modello centralizzato, Firewall Manager mantiene un singolo endpoint in un VPC di ispezione.
6. Per Regione, scegli un. Regione AWS Per proteggere le risorse in più regioni, devi creare politiche separate per ogni regione.
7. Seleziona Successivo.
8. Per Nome della politica, inserisci un nome descrittivo.
9. Nella configurazione della policy, scegli la policy firewall NGFW di Palo Alto Networks Cloud da associare a questa policy. L'elenco delle politiche firewall NGFW di Palo Alto Networks Cloud contiene tutte le politiche firewall Palo Alto Networks Cloud NGFW associate al tenant Palo Alto Networks Cloud NGFW. Per informazioni sulla creazione e la gestione delle policy firewall Palo Alto Networks Cloud NGFW, consulta la sezione Deploy Palo Alto Networks Cloud NGFW per l'argomento della guida all'implementazione di Palo Alto Networks Cloud NGFW. AWS AWS Firewall Manager AWS
10. Per la registrazione NGFW di Palo Alto Networks Cloud: opzionale, scegli facoltativamente quali tipi di log Palo Alto Networks Cloud NGFW registrare per la tua politica. Per informazioni sui tipi di log NGFW di Palo Alto Networks Cloud, consulta Configura la registrazione per Palo Alto Networks Cloud NGFW nella guida all'implementazione di Palo Alto Networks Cloud NGFW. AWS AWS

    Per la destinazione dei log, specificare in che momento Firewall Manager deve scrivere i log.

11. Seleziona Successivo.
12. In Configura un endpoint firewall di terze parti, esegui una delle seguenti operazioni, a seconda che utilizzi il modello di distribuzione distribuito o centralizzato per creare gli endpoint firewall:

    - Se utilizzi il modello di distribuzione distribuito per questa politica, in Zone di disponibilità, seleziona in quali zone di disponibilità creare gli endpoint del firewall. È possibile selezionare le zone di disponibilità in base al nome della zona di disponibilità o all'ID della zona di disponibilità.
    - Se utilizzi il modello di distribuzione centralizzato per questa policy, nella configurazione degli AWS Firewall Manager endpoint in configurazione Inspection VPC, inserisci l'ID AWS account del proprietario del VPC di ispezione e l'ID VPC del VPC di ispezione.
        - In Zone di disponibilità, seleziona le zone di disponibilità in cui creare gli endpoint del firewall. È possibile selezionare le zone di disponibilità in base al nome della zona di disponibilità o all'ID della zona di disponibilità.
13. Se desideri fornire i blocchi CIDR a Firewall Manager da utilizzare per le sottoreti firewall nei tuoi VPC, devono essere tutti blocchi CIDR /28. Inserisci un blocco per riga. Se li ometti, Firewall Manager sceglie gli indirizzi IP per te tra quelli disponibili nei VPC.

    > **Note**
    >
    > La riparazione automatica viene eseguita automaticamente per le politiche del AWS Firewall Manager Network Firewall, quindi qui non è disponibile un'opzione per scegliere di non eseguire la riparazione automatica.

14. Seleziona Successivo.
15. Nell'ambito della policy, ai sensi di Account AWS questa policy si applica a, scegli l'opzione seguente:

    - Se desideri applicare la politica a tutti gli account della tua organizzazione, lascia la selezione predefinita Includi tutti gli account della mia AWS organizzazione.
    - Se desideri applicare la politica solo a conti specifici o account appartenenti a unità AWS Organizations organizzative (OU) specifiche, scegli Includi solo gli account e le unità organizzative specificati, quindi aggiungi gli account e le unità organizzative che desideri includere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

- Se desideri applicare la politica a tutti i conti o le unità AWS Organizations organizzative (OU) tranne uno specifico, scegli Escludi gli account e le unità organizzative specificati e includi tutti gli altri, quindi aggiungi gli account e le unità organizzative che desideri escludere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

È possibile scegliere solo una delle opzioni.

Dopo aver applicato la policy, Firewall Manager valuta automaticamente tutti i nuovi account in base alle impostazioni dell'utente. Ad esempio, se includi solo account specifici, Firewall Manager non applica la politica a nessun nuovo account. Come altro esempio, se si include un'unità organizzativa, quando si aggiunge un account all'unità organizzativa o a una delle relative unità organizzative secondarie, Firewall Manager applica automaticamente la politica al nuovo account.

16. Il tipo di risorsa per le politiche del Network Firewall è VPC.
17. In Resources (Risorse), se si desidera proteggere (o escludere) solo le risorse con tag specifici, selezionare l'opzione appropriata, quindi immettere i tag da includere o escludere. È possibile scegliere una sola opzione. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .

    Se si immettono più tag, una risorsa deve avere tutti i tag da includere o escludere.
18. Per Concedi l'accesso a più account, scegli Scarica AWS CloudFormation modello. In questo modo viene scaricato un AWS CloudFormation modello che puoi utilizzare per creare uno AWS CloudFormation stack. Questo stack crea un AWS Identity and Access Management ruolo che concede a Firewall Manager le autorizzazioni per più account per gestire le risorse NGFW di Palo Alto Networks Cloud. Per informazioni sugli stack, consulta Working with stacks nella Guida per l'utente.AWS CloudFormation
19. Seleziona Successivo.
20. Per i tag Policy, aggiungi tutti i tag identificativi che desideri per la policy di Firewall Manager. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .
21. Seleziona Successivo.
22. Rivedere la nuova policy. Per apportare eventuali modifiche, scegliere Edit (Modifica) nell'area che si desidera modificare. In questo modo si torna al passaggio corrispondente della creazione guidata. Al termine, scegliere Create policy (Crea policy).

Creazione di una AWS Firewall Manager policy per Fortigate Cloud Native Firewall (CNF) as a Service

Con una policy Firewall Manager per Fortigate CNF, puoi utilizzare Firewall Manager per distribuire e gestire le risorse Fortigate CNF su tutti i tuoi account. AWS

Per informazioni sulle politiche CNF di Firewall Manager Fortigate, vedere. Politiche di Fortigate Cloud Native Firewall (CNF) as a Service Per informazioni su come configurare Fortigate CNF per l'uso con Firewall Manager, consulta la documentazione di Fortinet.

Prerequisiti

Vi sono diversi passaggi obbligatori per preparare l'account AWS Firewall Manager. Tali fasi sono descritte nell'articolo AWS Firewall Manager prerequisiti. Completa tutti i prerequisiti prima di procedere al passaggio successivo.

Per creare una policy Firewall Manager per Fortigate CNF (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Scegli Crea policy.
4. Per il tipo di policy, scegli Fortigate Cloud Native Firewall (CNF) as a Service. Se non ti sei ancora abbonato al servizio Fortigate CNF nel AWS Marketplace, devi prima farlo. Per iscriverti al AWS Marketplace, scegli Visualizza i dettagli del AWS Marketplace.
5. Per il modello di implementazione, scegli il modello distribuito o il modello centralizzato. Il modello di distribuzione determina il modo in cui Firewall Manager gestisce gli endpoint per la policy. Con il modello distribuito, Firewall Manager mantiene gli endpoint del firewall in ogni VPC che rientra nell'ambito delle policy. Con il modello centralizzato, Firewall Manager mantiene un singolo endpoint in un VPC di ispezione.

6. Per Regione, scegli un. Regione AWS Per proteggere le risorse in più regioni, devi creare politiche separate per ogni regione.
7. Seleziona Successivo.
8. Per Nome della politica, inserisci un nome descrittivo.
9. Nella configurazione della policy, scegli la policy firewall Fortigate CNF da associare a questa policy. L'elenco delle politiche firewall di Fortigate CNF contiene tutte le politiche firewall Fortigate CNF associate al tenant di Fortigate CNF. Per informazioni sulla creazione e la gestione dei tenant CNF di Fortigate, consulta la documentazione di Fortinet.
10. Seleziona Successivo.
11. In Configura un endpoint firewall di terze parti, esegui una delle seguenti operazioni, a seconda che tu stia utilizzando il modello di distribuzione distribuito o centralizzato per creare gli endpoint firewall:

    - Se utilizzi il modello di distribuzione distribuito per questa politica, in Zone di disponibilità, seleziona in quali zone di disponibilità creare gli endpoint del firewall. È possibile selezionare le zone di disponibilità in base al nome della zona di disponibilità o all'ID della zona di disponibilità.
    - Se utilizzi il modello di distribuzione centralizzato per questa policy, nella configurazione degli AWS Firewall Manager endpoint in configurazione Inspection VPC, inserisci l'ID AWS account del proprietario del VPC di ispezione e l'ID VPC del VPC di ispezione.
        - In Zone di disponibilità, seleziona le zone di disponibilità in cui creare gli endpoint del firewall. È possibile selezionare le zone di disponibilità in base al nome della zona di disponibilità o all'ID della zona di disponibilità.
12. Se desideri fornire i blocchi CIDR a Firewall Manager da utilizzare per le sottoreti firewall nei tuoi VPC, devono essere tutti blocchi CIDR /28. Inserisci un blocco per riga. Se li ometti, Firewall Manager sceglie gli indirizzi IP per te tra quelli disponibili nei VPC.

    > **Note**
    >
    > La riparazione automatica viene eseguita automaticamente per le politiche del AWS Firewall Manager Network Firewall, quindi qui non è disponibile un'opzione per scegliere di non eseguire la riparazione automatica.

13. Seleziona Successivo.

14. Nell'ambito della policy, ai sensi di Account AWS questa policy si applica a, scegli l'opzione seguente:

    - Se desideri applicare la politica a tutti gli account della tua organizzazione, lascia la selezione predefinita Includi tutti gli account della mia AWS organizzazione.
    - Se desideri applicare la politica solo a conti specifici o account appartenenti a unità AWS Organizations organizzative (OU) specifiche, scegli Includi solo gli account e le unità organizzative specificati, quindi aggiungi gli account e le unità organizzative che desideri includere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.
    - Se desideri applicare la politica a tutti i conti o le unità AWS Organizations organizzative (OU) tranne uno specifico, scegli Escludi gli account e le unità organizzative specificati e includi tutti gli altri, quindi aggiungi gli account e le unità organizzative che desideri escludere. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in ognuna delle unità organizzative figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.

    È possibile scegliere solo una delle opzioni.

    Dopo aver applicato la policy, Firewall Manager valuta automaticamente tutti i nuovi account in base alle impostazioni dell'utente. Ad esempio, se includi solo account specifici, Firewall Manager non applica la politica a nessun nuovo account. Come altro esempio, se si include un'unità organizzativa, quando si aggiunge un account all'unità organizzativa o a una delle relative unità organizzative secondarie, Firewall Manager applica automaticamente la politica al nuovo account.
15. Il tipo di risorsa per le politiche del Network Firewall è VPC.
16. In Resources (Risorse), se si desidera proteggere (o escludere) solo le risorse con tag specifici, selezionare l'opzione appropriata, quindi immettere i tag da includere o escludere. È possibile scegliere una sola opzione. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .

    Se si immettono più tag, una risorsa deve avere tutti i tag da includere o escludere.
17. Per Concedi l'accesso a più account, scegli Scarica AWS CloudFormation modello. In questo modo viene scaricato un AWS CloudFormation modello che puoi utilizzare per creare uno AWS CloudFormation stack. Questo stack crea un AWS Identity and Access Management ruolo che

concede a Firewall Manager le autorizzazioni per più account per gestire le risorse Fortigate CNF. Per informazioni sugli stack, consulta Working with stacks nella Guida per l'utente.AWS CloudFormation Per creare uno stack, è necessario l'ID dell'account dal portale Fortigate CNF.

18. Seleziona Successivo.
19. Per i tag Policy, aggiungi tutti i tag identificativi che desideri per la policy di Firewall Manager. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .
20. Seleziona Successivo.
21. Rivedere la nuova policy. Per apportare eventuali modifiche, scegliere Edit (Modifica) nell'area che si desidera modificare. In questo modo si torna al passaggio corrispondente della creazione guidata. Al termine, scegliere Create policy (Crea policy).

Eliminazione di un criterio AWS Firewall Manager

È possibile eliminare una policy Firewall Manager procedendo nel seguente modo.

Per eliminare una policy (console)

1. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
2. Scegliere l'opzione accanto alla policy da eliminare.
3. Scegli Elimina.

> **Note**
>
> Quando elimini una policy del gruppo di sicurezza comune di Firewall Manager, per rimuovere i gruppi di sicurezza di replica della policy, scegli l'opzione per ripulire le risorse create dalla policy. Altrimenti, dopo l'eliminazione del primario, le repliche rimangono e richiedono la gestione manuale in ogni istanza Amazon VPC.

> **Important**
>
> Quando elimini una policy di Firewall Manager Shield Advanced, la policy viene eliminata, ma i tuoi account rimangono abbonati a Shield Advanced.

AWS Firewall Manager ambito della politica

L'ambito della politica definisce dove si applica la politica. È possibile applicare politiche controllate centralmente a tutti gli account e le risorse all'interno dell'organizzazione o a un sottoinsieme di account e risorse. AWS Organizations Per istruzioni su come impostare l'ambito delle politiche, consultaCreazione di una AWS Firewall Manager politica.

Opzioni relative all'ambito delle politiche in AWS Firewall Manager

Quando si aggiunge un nuovo account o una nuova risorsa all'organizzazione, Firewall Manager lo valuta automaticamente in base alle impostazioni di ciascun criterio e applica il criterio in base a tali impostazioni. Ad esempio, è possibile scegliere di applicare un criterio a tutti gli account tranne i numeri di account in un elenco specificato; è anche possibile scegliere di applicare un criterio solo alle risorse che hanno tutti i tag in un elenco.

Account AWS nell'ambito

Le impostazioni fornite per definire gli Account AWS interessati dalla politica determinano a quali account dell' AWS organizzazione applicare la politica. È possibile scegliere di applicare il criterio in uno dei seguenti modi:

- A tutti gli account nell'organizzazione
- Solo a un elenco specifico di numeri di account e unità organizzative AWS Organizations inclusi
- A tutti tranne a un elenco specifico di numeri di account e unità organizzative AWS Organizations escluse

Per informazioni in merito AWS Organizations, consulta la Guida AWS Organizations per l'utente.

Risorse nell'ambito di applicazione

Analogamente alle impostazioni per gli account inclusi nell'ambito, le impostazioni fornite per le risorse determinano a quali tipi di risorse nell'ambito applicare la politica. È possibile scegliere una delle seguenti opzioni:

- Tutte le risorse
- Risorse con tutti i tag specificati
- Tutte le risorse tranne quelle che hanno tutti i tag specificati

Per ulteriori informazioni sull'assegnazione di tag alle risorse, vedere Utilizzo dell'editor dei tag.

Gestione dell'ambito delle politiche in AWS Firewall Manager

Quando le policy sono in vigore, Firewall Manager le gestisce continuamente e le applica a nuove Account AWS risorse man mano che vengono aggiunte, in base all'ambito della policy.

Gestione Account AWS e risorse di Firewall Manager

Se un account o una risorsa non rientra nell'ambito di applicazione per qualsiasi motivo, AWS Firewall Manager non rimuove automaticamente le protezioni o elimina le risorse gestite da Firewall Manager a meno che non si selezioni la casella di controllo Rimuovi automaticamente le protezioni dalle risorse che esulano dall'ambito della policy.

> **Note**
>
> L'opzione Rimuovi automaticamente le protezioni dalle risorse che esulano dall'ambito della policy non è disponibile per le policy classiche. AWS Shield Advanced AWS WAF

La selezione di questa casella di controllo consente di AWS Firewall Manager ripulire automaticamente le risorse gestite da Firewall Manager per gli account quando tali account escono dall'ambito delle politiche. Ad esempio, Firewall Manager dissocierà un ACL Web gestito da Firewall Manager da una risorsa cliente protetta quando la risorsa cliente esce dall'ambito della policy.

Per determinare quali risorse devono essere rimosse dalla protezione quando una risorsa del cliente esce dall'ambito delle policy, Firewall Manager segue queste linee guida:

- Comportamento predefinito:
  - Le regole AWS Config gestite associate vengono eliminate. Questo comportamento è indipendente dalla casella di controllo.
  - Tutti gli elenchi di controllo degli accessi AWS WAF Web associati (ACL Web) che non contengono risorse vengono eliminati. Questo comportamento è indipendente dalla casella di controllo.
  - Qualsiasi risorsa protetta che non rientra nell'ambito di applicazione rimane associata e protetta. Ad esempio, un Application Load Balancer o un'API di API Gateway associata a un ACL Web rimane associata all'ACL Web e la protezione rimane valida.
- Con la casella di controllo Rimuovi automaticamente le protezioni dalle risorse che esulano dall'ambito della policy selezionata:

- Le regole AWS Config gestite associate vengono eliminate. Questo comportamento è indipendente dalla casella di controllo.
- Tutti gli elenchi di controllo degli accessi AWS WAF Web associati (ACL Web) che non contengono risorse vengono eliminati. Questo comportamento è indipendente dalla casella di controllo.
- Qualsiasi risorsa protetta che non rientra nell'ambito di applicazione viene automaticamente dissociata e rimossa dalla protezione quando esce dall'ambito della policy. Ad esempio, un acceleratore Elastic Inference o un'istanza Amazon EC2 viene automaticamente dissociata dal gruppo di sicurezza replicato quando esce dall'ambito della policy. Il gruppo di sicurezza replicato e le relative risorse vengono automaticamente rimossi dalla protezione.

Elenchi gestiti

Gli elenchi gestiti di applicazioni e protocolli semplificano la configurazione e la gestione delle politiche dei gruppi di sicurezza per il controllo dei AWS Firewall Manager contenuti. Gli elenchi gestiti vengono utilizzati per definire i protocolli e le applicazioni consentiti e non consentiti dalla policy. Per informazioni sulle politiche dei gruppi di sicurezza di Content Audit, vederePolicy di gruppo di sicurezza del controllo dei contenuti.

È possibile utilizzare i seguenti tipi di elenchi gestiti in una politica di gruppo di sicurezza per il controllo dei contenuti:

- Elenchi di applicazioni e protocolli di Firewall Manager: Firewall Manager gestisce questi elenchi.
  - Gli elenchi di applicazioni includono `FMS-Default-Public-Access-Apps-Allowed` e`FMS-Default-Public-Access-Apps-Denied`, che descrivono le applicazioni di uso comune che dovrebbero essere consentite o negate al pubblico in generale.
  - Gli elenchi dei protocolli includono `FMS-Default-Protocols-Allowed` un elenco di protocolli di uso comune che dovrebbero essere consentiti al pubblico in generale. È possibile utilizzare qualsiasi elenco gestito da Firewall Manager, ma non è possibile modificarlo o eliminarlo.
- Elenchi di applicazioni ed elenchi di protocolli personalizzati: questi elenchi sono gestiti dall'utente. È possibile creare elenchi di entrambi i tipi con le impostazioni necessarie. Hai il pieno controllo sui tuoi elenchi gestiti personalizzati e puoi crearli, modificarli ed eliminarli secondo necessità.

> **Note**
>
> Attualmente, Firewall Manager non controlla i riferimenti a un elenco gestito personalizzato quando lo elimini. Ciò significa che è possibile eliminare un elenco di applicazioni gestite personalizzato o un elenco di protocolli anche quando è utilizzato da una policy attiva. Ciò può causare l'interruzione del funzionamento della politica. Eliminate un elenco di applicazioni o un elenco di protocolli solo dopo aver verificato che nessuna policy attiva vi faccia riferimento.

Gli elenchi gestiti sono risorse AWS . È possibile contrassegnare un elenco gestito personalizzato. Non è possibile aggiungere tag a un elenco gestito di Firewall Manager.

Controllo delle versioni gestite degli elenchi

Gli elenchi gestiti personalizzati non hanno versioni. Quando si modifica un elenco personalizzato, i criteri che fanno riferimento all'elenco utilizzano automaticamente l'elenco aggiornato.

Gli elenchi gestiti di Firewall Manager hanno una versione. Il team di assistenza Firewall Manager pubblica nuove versioni in base alle esigenze, al fine di applicare le migliori pratiche di sicurezza agli elenchi.

Quando si utilizza un elenco gestito di Firewall Manager in una policy, si sceglie la strategia di controllo delle versioni nel modo seguente:

- Ultima versione disponibile: se non si specifica un'impostazione di versione esplicita per l'elenco, la politica utilizza automaticamente la versione più recente. Questa è l'unica opzione disponibile tramite la console.
- Versione esplicita: se si specifica una versione per l'elenco, la politica utilizza tale versione. La politica rimane vincolata alla versione specificata fino a quando non si modifica l'impostazione della versione. Per specificare la versione, è necessario definire la policy all'esterno della console, ad esempio tramite la CLI o uno degli SDK.

Per ulteriori informazioni sulla scelta dell'impostazione della versione per un elenco, consulta. Utilizzo di elenchi gestiti nelle policy dei gruppi di sicurezza per il controllo dei contenuti

Utilizzo di elenchi gestiti nelle policy dei gruppi di sicurezza per il controllo dei contenuti

Quando crei una policy di gruppo per la sicurezza del controllo dei contenuti, puoi scegliere di utilizzare le regole della policy di controllo gestita. Alcune impostazioni di questa opzione richiedono un elenco di applicazioni gestite o un elenco di protocolli. Esempi di queste impostazioni includono i protocolli consentiti nelle regole dei gruppi di sicurezza e le applicazioni possono accedere a Internet.

Le seguenti restrizioni si applicano a ogni impostazione dei criteri che utilizza un elenco gestito:

- È possibile specificare al massimo un elenco gestito di Firewall Manager per qualsiasi impostazione. Per impostazione predefinita, è possibile specificare al massimo un elenco personalizzato. Il limite dell'elenco personalizzato è una quota fissa, quindi è possibile richiederne un aumento. Per ulteriori informazioni, consulta AWS Firewall Manager quote.
- Nella console, se si seleziona un elenco gestito di Firewall Manager, non è possibile specificare la versione. La policy utilizzerà sempre la versione più recente dell'elenco. Per specificare la versione, è necessario definire la policy all'esterno della console, ad esempio tramite la CLI o uno degli SDK. Per informazioni sul controllo delle versioni per gli elenchi gestiti di Firewall Manager, vedereControllo delle versioni gestite degli elenchi.

Per informazioni sulla creazione di una policy di gruppo di sicurezza per il controllo dei contenuti tramite la console, vedereCreazione di una policy di gruppo di sicurezza di controllo del contenuto.

Creazione di un elenco di applicazioni gestite personalizzato

Per creare un elenco di applicazioni gestite personalizzato

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegli Elenchi di applicazioni.
3. Nella pagina Elenchi di applicazioni, scegli Crea elenco di applicazioni.

4. Nella pagina Crea elenco di applicazioni, assegna un nome all'elenco. Non utilizzare il prefisso `fms-` poiché è riservato a Firewall Manager.
5. Specificate un'applicazione fornendo il protocollo e il numero di porta o selezionando un'applicazione dal menu a discesa Tipo. Assegna un nome alle specifiche dell'applicazione.
6. Scegli Aggiungi un altro se necessario e inserisci le informazioni sulla domanda fino a completare l'elenco.
7. (Facoltativo) Applica i tag all'elenco.
8. Scegli Salva per salvare l'elenco e tornare alla pagina degli elenchi di applicazioni.

Creazione di un elenco di protocolli gestiti personalizzato

Per creare un elenco di protocolli gestiti personalizzato

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegli Elenchi di protocolli.
3. Nella pagina degli elenchi dei protocolli, scegli Crea elenco di protocolli.
4. Nella pagina di creazione dell'elenco dei protocolli, assegna un nome alla lista. Non utilizzare il prefisso `fms-` poiché è riservato a Firewall Manager.
5. Specificare un protocollo.
6. Scegli Aggiungi un altro se necessario e inserisci le informazioni sul protocollo fino a completare l'elenco.
7. (Facoltativo) Applica i tag all'elenco.
8. Scegli Salva per salvare l'elenco e tornare alla pagina degli elenchi dei protocolli.

Visualizzazione di un elenco gestito

Per visualizzare un elenco di applicazioni o un elenco di protocolli

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegli Elenchi di applicazioni o Elenchi di protocolli.

   La pagina mostra tutti gli elenchi del tipo selezionato disponibili per l'uso. Gli elenchi gestiti da Firewall Manager hanno una Y nella ManagedListcolonna.

3. Per visualizzare i dettagli di un elenco, scegline il nome. La pagina dei dettagli mostra il contenuto dell'elenco e gli eventuali tag.

   Per gli elenchi gestiti di Firewall Manager, puoi anche vedere le versioni disponibili selezionando il menu a discesa Versione.

Eliminazione di un elenco gestito personalizzato

È possibile eliminare elenchi gestiti personalizzati. Non è possibile modificare o eliminare gli elenchi gestiti da Firewall Manager.

> **Note**
>
> Attualmente, Firewall Manager non controlla i riferimenti a un elenco gestito personalizzato quando lo elimini. Ciò significa che è possibile eliminare un elenco di applicazioni gestite personalizzato o un elenco di protocolli anche quando è utilizzato da una policy attiva. Ciò può causare l'interruzione del funzionamento della politica. Elimina un elenco di applicazioni o un elenco di protocolli solo dopo aver verificato che nessuna policy attiva vi faccia riferimento.

Per eliminare un'applicazione gestita personalizzata o un elenco di protocolli

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Assicurati che l'elenco che desideri eliminare non sia utilizzato in nessuna delle policy dei tuoi gruppi di sicurezza di controllo procedendo come segue:

   a. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).

   b. Nella pagina delle AWS Firewall Manager politiche, seleziona e modifica i gruppi di sicurezza di controllo e rimuovi tutti i riferimenti all'elenco personalizzato che desideri eliminare.

      Se elimini un elenco gestito personalizzato utilizzato in una politica di gruppo di sicurezza di controllo, la politica che lo utilizza può smettere di funzionare.

3. Nel riquadro di navigazione, scegli Elenchi di applicazioni o Elenchi di protocolli, a seconda del tipo di elenco che desideri eliminare.

4. Nella pagina dell'elenco, seleziona l'elenco personalizzato che desideri eliminare e scegli Elimina.

AWS WAF politiche

In una AWS WAF politica di Firewall Manager, si specificano i gruppi di AWS WAF regole che si desidera utilizzare tra le risorse. Quando si applica la policy, Firewall Manager crea ACL Web negli account che rientrano nell'ambito della policy, a seconda di come si configura la gestione degli ACL Web nella policy. Negli ACL Web creati dalla policy, i singoli account manager possono aggiungere regole e gruppi di regole, oltre ai gruppi di regole definiti tramite Firewall Manager.

In che modo Firewall Manager gestisce gli ACL Web

Firewall Manager crea ACL Web in base a come configuri l'impostazione Gestisci ACL Web non associati nella tua politica o l'`optimizeUnassociatedWebACL`impostazione nel tipo di SecurityServicePolicyDatadati nell'API.

Se si abilita la gestione degli ACL Web non associati, Firewall Manager crea ACL Web negli account rientranti nell'ambito delle policy solo se gli ACL Web verranno utilizzati da almeno una risorsa. Se in qualsiasi momento un account rientra nell'ambito delle politiche, Firewall Manager crea automaticamente un ACL Web nell'account se almeno una risorsa utilizzerà l'ACL Web. Quando abiliti la gestione degli ACL Web non associati, Firewall Manager esegue una pulizia una tantum degli ACL Web non associati nel tuo account. Durante la pulizia, Firewall Manager ignora tutti gli ACL Web modificati dopo la loro creazione, ad esempio se hai aggiunto un gruppo di regole all'ACL Web o ne hai modificato le impostazioni. Il processo di pulizia può richiedere diverse ore. Se una risorsa esce dall'ambito delle policy dopo che Firewall Manager ha creato un ACL Web, Firewall Manager dissocia la risorsa dall'ACL Web, ma non ripulisce l'ACL Web non associato. Firewall Manager pulisce gli ACL Web non associati solo quando si abilita per la prima volta la gestione degli ACL Web non associati in una policy.

Se non si abilita questa opzione, Firewall Manager non gestisce gli ACL Web non associati e Firewall Manager crea automaticamente un ACL Web in ogni account che rientra nell'ambito delle policy.

Campionamento e metriche CloudWatch

AWS Firewall Manager abilita il campionamento e i CloudWatch parametri Amazon per gli ACL Web e i gruppi di regole che crea per una policy. AWS WAF

Struttura di denominazione ACL Web

Quando Firewall Manager crea un ACL Web per la policy, assegna un nome all'`FMManagedWebACLV2-`*`policy name`*`-`*`timestamp`*ACL Web. Il timestamp è in millisecondi UTC. Ad esempio, `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`.

> **Note**
>
> Se una risorsa configurata con la mitigazione automatica avanzata degli attacchi DDoS a livello di applicazione rientra nell'ambito di una AWS WAF policy, Firewall Manager non sarà in grado di associare l'ACL Web creato dalla AWS WAF policy alla risorsa.

Gruppi di regole nelle politiche AWS WAF

Gli ACL Web gestiti dalle AWS WAF politiche di Firewall Manager contengono tre set di regole. Questi set forniscono un livello più elevato di priorità per le regole e i gruppi di regole nell'ACL Web:

- Primi gruppi di regole, definiti dall'utente nella AWS WAF politica di Firewall Manager. AWS WAF valuta prima questi gruppi di regole.
- Regole e gruppi di regole definiti dai responsabili dell'account nelle ACL Web. AWS WAF valuta successivamente le regole gestite dall'account o i gruppi di regole.
- Ultimi gruppi di regole, definiti dall'utente nella AWS WAF politica di Firewall Manager. AWS WAF valuta questi gruppi di regole per ultimi.

All'interno di ciascuno di questi set di regole, AWS WAF valuta le regole e i gruppi di regole come di consueto, in base alle relative impostazioni di priorità all'interno del set.

Nel primo e nell'ultimo set di gruppi di regole della policy è possibile aggiungere solo gruppi di regole. Puoi utilizzare i gruppi di regole gestiti, che AWS Managed Rules e Marketplace AWS i venditori creano e gestiscono per te. È inoltre possibile gestire e utilizzare propri gruppi di regole. Per ulteriori informazioni su tutte queste opzioni, consulta Gruppi di regole.

Se desideri utilizzare i tuoi gruppi di regole, creali prima di creare la AWS WAF policy di Firewall Manager. Per le linee guida, consulta Gestione dei propri gruppi di regole. Per utilizzare una singola regola personalizzata, è necessario definire il proprio gruppo di regole, definire la regola all'interno del gruppo e quindi utilizzare il gruppo di regole nella policy.

Il primo e l'ultimo gruppo di AWS WAF regole gestiti tramite Firewall Manager hanno nomi che iniziano con `PREFMManaged-` o `POSTFMManaged-`, rispettivamente, seguiti dal nome della policy di Firewall Manager e dal timestamp di creazione del gruppo di regole, in millisecondi UTC. Ad esempio, `PREFMManaged-MyWAFPolicyName-1621880555123`.

Per informazioni su come valuta le richieste Web, vedere AWS WAF . Valutazione delle regole ACL Web e dei gruppi di regole

Per la procedura di creazione di una AWS WAF policy di Firewall Manager, vedereCreazione di una AWS Firewall Manager politica per AWS WAF.

Firewall Manager consente il campionamento e i CloudWatch parametri Amazon per i gruppi di regole definiti per la AWS WAF policy.

I proprietari di account individuali hanno il controllo completo sulle metriche e sulla configurazione di campionamento per qualsiasi regola o gruppo di regole che aggiungono agli ACL web gestiti della policy.

Configurazione della registrazione per una policy AWS WAF

Puoi abilitare la registrazione centralizzata per AWS WAF le tue politiche per ottenere informazioni dettagliate sul traffico analizzato dall'ACL web all'interno dell'organizzazione. Le informazioni contenute nei log includono l'ora in cui è AWS WAF stata ricevuta la richiesta dalla AWS risorsa, informazioni dettagliate sulla richiesta e l'azione applicata alla regola secondo cui ogni richiesta corrisponde per tutti gli account interessati. Puoi inviare i log a un flusso di dati Amazon Data Firehose o a un bucket Amazon Simple Storage Service (S3). Per informazioni sulla AWS WAF registrazione, consulta Registrazione del traffico AWS WAF ACL Web la Guida per gli sviluppatori.AWS WAF

> **Note**
>
> AWS Firewall Manager supporta questa opzione per AWS WAFV2, non per AWS WAF Classic.

Argomenti

- Destinazioni di registrazione
- Abilitazione della registrazione
- Disattivazione della registrazione

Destinazioni di registrazione

Questa sezione descrive le destinazioni di registrazione che è possibile scegliere per inviare i registri delle AWS WAF politiche. Ogni sezione fornisce indicazioni per configurare la registrazione per il tipo di destinazione e informazioni su qualsiasi comportamento specifico del tipo di destinazione. Dopo aver configurato la destinazione di registrazione, puoi fornire le relative specifiche alla AWS WAF politica di Firewall Manager per iniziare a registrarla.

Firewall Manager non ha visibilità sugli errori di registro dopo la creazione della configurazione di registrazione. È tua responsabilità verificare che la consegna dei log funzioni come previsto.

> **Note**
>
> Firewall Manager non modifica alcuna configurazione di registrazione esistente negli account dei membri dell'organizzazione.

Argomenti

- Flussi di dati Amazon Data Firehose
- Bucket Amazon Simple Storage Service

Flussi di dati Amazon Data Firehose

Questo argomento fornisce informazioni per inviare i log di traffico ACL Web a un flusso di dati Amazon Data Firehose.

Quando abiliti la registrazione di Amazon Data Firehose, Firewall Manager invia i log dagli ACL Web della tua policy a un Amazon Data Firehose in cui hai configurato una destinazione di storage. Dopo aver abilitato la registrazione, AWS WAF invia i log per ogni ACL Web configurato, tramite l'endpoint HTTPS di Kinesis Data Firehose alla destinazione di archiviazione configurata. Prima di utilizzarlo, verifica il flusso di distribuzione per assicurarti che abbia un throughput sufficiente per contenere i log della tua organizzazione. Per ulteriori informazioni su come creare un Amazon Kinesis Data Firehose e rivedere i log memorizzati, consulta What Is Amazon Data Firehose?

È necessario disporre delle seguenti autorizzazioni per abilitare correttamente la registrazione con Kinesis:

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

Quando configuri una destinazione di registrazione di Amazon Data Firehose su una AWS WAF policy, Firewall Manager crea un ACL web per la policy nell'account amministratore di Firewall Manager come segue:

- Firewall Manager crea l'ACL Web nell'account amministratore di Firewall Manager indipendentemente dal fatto che l'account rientri nell'ambito della politica.

- L'ACL Web ha la registrazione abilitata, con un nome di registro`FMManagedWebACLV2-Logging`*`policy name`*`-`*`timestamp`*, dove il timestamp è l'ora UTC in cui il registro è stato abilitato per l'ACL Web, in millisecondi. Ad esempio, `FMManagedWebACLV2-LoggingMyWAFPolicyName-1621880565180`. L'ACL web non ha gruppi di regole né risorse associate.
- L'ACL web ti viene addebitato in base alle linee guida sui AWS WAF prezzi. Per ulteriori informazioni, consulta la sezione Prezzi di AWS WAF.
- Firewall Manager elimina l'ACL Web quando si elimina la policy.

Per informazioni sui ruoli collegati ai servizi e sull'autorizzazione, vedere. `iam:CreateServiceLinkedRole` Utilizzo di ruoli collegati ai servizi per AWS WAF

Per ulteriori informazioni sulla creazione di un flusso di distribuzione, consulta Creating an Amazon Data Firehose Delivery Stream.

Bucket Amazon Simple Storage Service

Questo argomento fornisce informazioni per inviare i log di traffico ACL Web a un bucket Amazon S3.

Il bucket scelto come destinazione di registrazione deve appartenere a un account amministratore di Firewall Manager. Per informazioni sui requisiti per la creazione del bucket Amazon S3 per la registrazione e i requisiti di denominazione dei bucket, consulta Amazon Simple Storage Service nella Developer Guide.AWS WAF

Consistenza finale

Quando apporti modifiche alle AWS WAF politiche configurate con una destinazione di registrazione Amazon S3, Firewall Manager aggiorna la policy del bucket per aggiungere le autorizzazioni necessarie per la registrazione. A tale scopo, Firewall Manager segue i modelli di last-writer-wins semantica e coerenza dei dati seguiti da Amazon Simple Storage Service. Se effettui contemporaneamente più aggiornamenti delle policy a una destinazione Amazon S3 nella console Firewall Manager o tramite PutPolicyl'API, alcune autorizzazioni potrebbero non essere salvate. Per ulteriori informazioni sul modello di coerenza dei dati di Amazon S3, consulta il modello di coerenza dei dati di Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

Autorizzazioni per pubblicare i log in un bucket Amazon S3

La configurazione della registrazione del traffico Web ACL per un bucket Amazon S3 in una AWS WAF policy richiede le seguenti impostazioni di autorizzazione. Firewall Manager assegna

automaticamente queste autorizzazioni al tuo bucket Amazon S3 quando configuri Amazon S3 come destinazione di registrazione per concedere al servizio l'autorizzazione a pubblicare i log nel bucket. Se desideri gestire un accesso più dettagliato alle tue risorse di registrazione e Firewall Manager, puoi impostare tu stesso queste autorizzazioni. Per informazioni sulla gestione delle autorizzazioni, consulta Gestione degli accessi alle AWS risorse nella Guida per l'utente IAM. Per informazioni sulle politiche AWS WAF gestite, consultaAWS politiche gestite per 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-example-bucket"
        },
        {
            "Sid": "AWSLogDeliveryWriteFMS",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::aws-waf-logs-example-bucket/policy-id/AWSLogs/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

Per evitare il problema della confusione tra diversi servizi, puoi aggiungere le chiavi relative al `aws:SourceArn`contesto della condizione `aws:SourceAccount`globale alla policy del tuo bucket. Per aggiungere queste chiavi, puoi modificare la policy che Firewall Manager crea automaticamente quando configuri la destinazione di registrazione oppure, se desideri un controllo granulare, puoi

creare una policy personalizzata. Se aggiungi queste condizioni alla tua politica di destinazione della registrazione, Firewall Manager non convaliderà né monitorerà le confuse protezioni sostitutive. Per informazioni generali sul problema del vice confuso, vedi Il problema del vice confuso nella Guida per l'utente di IAM.

Quando `sourceAccount` aggiungi le `sourceArn` proprietà di aggiunta, aumenterai la dimensione della policy del bucket. Se stai aggiungendo un lungo elenco di `sourceArn` proprietà di `sourceAccount` aggiunta, fai attenzione a non superare la quota di dimensione della policy del bucket Amazon S3.

L'esempio seguente mostra come prevenire il confuso problema vice utilizzando le chiavi di contesto `aws:SourceArn` e `aws:SourceAccount` global condition nella policy del bucket. Sostituiscili *`member-account-id`*con gli ID degli account dei membri della tua organizzazione.

```
{
   "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-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-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:*"
               ]
            }
         }
      }
   ]
}
```

Crittografia lato server per bucket Amazon S3

Puoi abilitare la crittografia lato server di Amazon S3 o utilizzare una chiave gestita AWS Key Management Service dal cliente sul tuo bucket S3. Se scegli di utilizzare la crittografia Amazon S3 predefinita sul tuo bucket Amazon S3 AWS WAF per i log, non devi intraprendere alcuna azione speciale. Tuttavia, se scegli di utilizzare una chiave di crittografia fornita dal cliente per crittografare i dati inattivi di Amazon S3, devi aggiungere la seguente dichiarazione di autorizzazione alla tua politica di chiave: AWS Key Management Service

```
{
            "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": "*"
}
```

Per informazioni sull'utilizzo delle chiavi di crittografia fornite dal cliente con Amazon S3, consulta Uso della crittografia lato server con chiavi fornite dal cliente (SSE-C) nella Guida per l'utente di Amazon Simple Storage Service.

Abilitazione della registrazione

La procedura seguente descrive come abilitare la registrazione per una AWS WAF policy nella console Firewall Manager.

Per abilitare la registrazione per una politica AWS WAF

1. Prima di poter abilitare la registrazione, è necessario configurare le risorse di destinazione della registrazione come segue:

   - Amazon Kinesis Data Streams: crea un Amazon Data Firehose utilizzando il tuo account amministratore di Firewall Manager. Usa un nome che inizia con il prefisso. `aws-waf-logs-` Ad esempio, `aws-waf-logs-firewall-manager-central`. Crea il data firehose con una PUT fonte e nella regione in cui stai operando. Se stai acquisendo log per Amazon CloudFront, crea la firehose negli Stati Uniti orientali (Virginia settentrionale). Prima di utilizzarlo, verifica il flusso di distribuzione per assicurarti che abbia una velocità di trasmissione sufficiente per contenere i log della tua organizzazione. Per ulteriori informazioni, consulta Creazione di un flusso di distribuzione Amazon Data Firehose.
   - Bucket Amazon Simple Storage Service: crea un bucket Amazon S3 in base alle linee guida nell'argomento Amazon Simple Storage Service nella AWS WAF Developer Guide. È inoltre necessario configurare il bucket Amazon S3 con le autorizzazioni elencate in. Autorizzazioni per pubblicare i log in un bucket Amazon S3

2. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

> **Note**
>
> Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

3. Nel riquadro di navigazione, scegli Politiche di sicurezza.
4. Scegli la AWS WAF politica per cui desideri abilitare la registrazione. Per ulteriori informazioni sulla registrazione di AWS WAF , consulta Registrazione del traffico AWS WAF ACL Web.
5. Nella scheda Dettagli della politica, nella sezione Regole della politica, scegli Modifica.
6. Per la configurazione della registrazione, scegli Abilita registrazione per attivare la registrazione. La registrazione fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. Scegli la destinazione di registrazione, quindi scegli la destinazione di registrazione che hai configurato. È necessario scegliere una destinazione di registrazione il cui nome inizi con. `aws-waf-logs-` Per informazioni sulla configurazione di una destinazione di AWS WAF registrazione, vedere. Configurazione della registrazione per una policy AWS WAF
7. (Facoltativo) Se non si desidera che determinati campi e i relativi valori vengano inclusi nei log, omettere tali campi. Scegliere il campo da omettere, quindi selezionare Add (Aggiungi). Se necessario, ripetere l'operazione per omettere i campi aggiuntivi. I campi omessi vengono visualizzati come `REDACTED` nei log. Ad esempio, se si oscura il campo URI, il campo URI nei registri sarà. `REDACTED`
8. (Facoltativo) Se non desideri inviare tutte le richieste ai log, aggiungi i criteri e il comportamento di filtro. In Filtra log, per ogni filtro che desideri applicare, scegli Aggiungi filtro, quindi scegli i criteri di filtro e specifica se desideri conservare o eliminare le richieste che corrispondono ai criteri. Al termine dell'aggiunta dei filtri, se necessario, modifica il comportamento di registrazione predefinito. Per ulteriori informazioni, consulta la sezione Gestione della registrazione per un ACL Web nella Guida per gli sviluppatori di AWS WAF .
9. Seleziona Successivo.
10. Controlla le impostazioni, quindi scegli Salva per salvare le modifiche alla politica.

Disattivazione della registrazione

La procedura seguente descrive come disabilitare la registrazione per una AWS WAF policy nella console Firewall Manager.

Per disabilitare la registrazione per una politica AWS WAF

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegli Politiche di sicurezza.
3. Scegli la AWS WAF politica per cui desideri disabilitare la registrazione.
4. Nella scheda Dettagli della politica, nella sezione Regole della politica, scegli Modifica.
5. Per lo stato di configurazione della registrazione, scegli Disabilitato.
6. Seleziona Successivo.
7. Controlla le impostazioni, quindi scegli Salva per salvare le modifiche alla politica.

AWS Shield Advanced politiche

In una AWS Shield politica di Firewall Manager, scegli le risorse che desideri proteggere. Quando si applica la policy con la riparazione automatica abilitata, per ogni risorsa dell'ambito che non è già associata a un ACL AWS WAF Web, Firewall Manager associa un ACL Web vuoto. AWS WAF L'ACL web vuoto viene utilizzato per scopi di monitoraggio Shield. Se poi si associa un altro ACL Web alla risorsa, Firewall Manager rimuove l'associazione ACL Web vuota.

> **Note**
>
> Quando una risorsa che rientra nell'ambito di una AWS WAF policy rientra nell'ambito di una policy Shield Advanced configurata con la mitigazione automatica degli attacchi DDoS a livello di applicazione, Firewall Manager applica la protezione Shield Advanced solo dopo aver associato l'ACL web creato dalla policy. AWS WAF

Come AWS Firewall Manager gestisce gli ACL Web non associati nelle politiche Shield

Puoi configurare se Firewall Manager gestisca gli ACL Web non associati per te tramite l'impostazione Gestisci ACL Web non associati nella tua politica o l'`optimizeUnassociatedWebACL`impostazione nel tipo di SecurityServicePolicyDatadati nell'API. Se nella policy si abilita la gestione degli ACL Web non associati, Firewall Manager crea ACL Web negli account che rientrano nell'ambito della policy solo se gli ACL Web verranno utilizzati da almeno una risorsa. Se in qualsiasi momento un account rientra nell'ambito delle politiche, Firewall Manager crea automaticamente un ACL Web nell'account se almeno una risorsa utilizzerà l'ACL Web.

Quando abiliti la gestione degli ACL Web non associati, Firewall Manager esegue una pulizia una tantum degli ACL Web non associati nel tuo account. Il processo di pulizia può richiedere diverse ore. Se una risorsa esce dall'ambito delle policy dopo che Firewall Manager ha creato un ACL Web, Firewall Manager non dissocia la risorsa dall'ACL Web. Se desideri che Firewall Manager pulisca l'ACL Web, devi prima dissociare manualmente le risorse dall'ACL Web e quindi abilitare l'opzione di gestione degli ACL Web non associati nella tua politica.

Se non si abilita questa opzione, Firewall Manager non gestisce gli ACL Web non associati e Firewall Manager crea automaticamente un ACL Web in ogni account che rientra nell'ambito delle policy.

Come AWS Firewall Manager gestisce le modifiche all'ambito nelle politiche Shield

Gli account e le risorse possono uscire dall'ambito di una politica AWS Firewall Manager Shield Advanced a causa di una serie di modifiche, come modifiche alle impostazioni dell'ambito dei criteri, modifiche ai tag su una risorsa e la rimozione di un account da un'organizzazione. Per informazioni generali sulle impostazioni degli ambiti delle politiche, vedereAWS Firewall Manager ambito della politica.

Con una policy AWS Firewall Manager Shield Advanced, se un account o una risorsa non rientra nell'ambito di applicazione, Firewall Manager interrompe il monitoraggio dell'account o della risorsa.

Se un account non rientra nell'ambito di applicazione a causa della rimozione dall'organizzazione, continuerà a essere sottoscritto a Shield Advanced. Poiché l'account non fa più parte della famiglia di fatturazione consolidata, all'account verrà addebitato un canone di abbonamento Shield Advanced ripartito proporzionalmente. D'altra parte, un account che non rientra nell'ambito di applicazione ma rimane nell'organizzazione non comporta costi aggiuntivi.

Se una risorsa non rientra nell'ambito di applicazione, continua a essere protetta da Shield Advanced e continua a essere soggetta ai costi di trasferimento dati Shield Advanced.

Mitigazione automatica degli attacchi DDoS a livello di applicazione

Quando applichi una policy Shield Advanced alle CloudFront distribuzioni Amazon o Application Load Balancers, hai la possibilità di configurare la mitigazione automatica degli attacchi DDoS a livello di applicazione Shield Advanced nella policy.

Per informazioni sulla mitigazione automatica Shield Advanced, vedereMitigazione DDoS automatica a livello di applicazione Shield Advanced.

La mitigazione automatica degli attacchi DDoS a livello di applicazione Shield Advanced presenta i seguenti requisiti:

- La mitigazione automatica degli attacchi DDoS a livello di applicazione funziona solo con le CloudFront distribuzioni Amazon e gli Application Load Balancer.

  Se applichi la tua politica Shield Advanced alle CloudFront distribuzioni Amazon, puoi scegliere questa opzione per le politiche Shield Advanced che crei per la regione globale. Se si applicano protezioni agli Application Load Balancer, è possibile applicare la policy a qualsiasi regione supportata da Firewall Manager.
- La mitigazione automatica degli attacchi DDoS a livello di applicazione funziona solo con gli ACL Web creati utilizzando l'ultima versione di (v2). AWS WAF

  Per questo motivo, se si dispone di una politica che utilizza gli ACL Web AWS WAF classici, è necessario sostituire la politica con una nuova politica, che utilizzerà automaticamente la versione più recente di AWS WAF, oppure fare in modo che Firewall Manager crei una nuova versione degli ACL Web per la politica esistente e passi a utilizzarli. Per ulteriori informazioni su queste opzioni, consulta Sostituisci gli ACL web AWS WAF classici con gli ACL web della versione più recente.

Configurazione automatica della mitigazione

L'opzione di mitigazione automatica degli attacchi DDoS a livello di applicazione per le policy di Firewall Manager Shield Advanced applica la funzionalità di mitigazione automatica Shield Advanced agli account e alle risorse pertinenti alla policy. Per informazioni dettagliate su questa funzionalità Shield Advanced, vedereMitigazione DDoS automatica a livello di applicazione Shield Advanced.

Puoi scegliere di abilitare o disabilitare Firewall Manager la mitigazione automatica per CloudFront le distribuzioni o gli Application Load Balancer che rientrano nell'ambito della policy, oppure puoi scegliere di fare in modo che la policy ignori le impostazioni di mitigazione automatica di Shield Advanced:

- Abilita: se scegli di abilitare la mitigazione automatica, specifichi anche se le regole di mitigazione di Shield Advanced devono contare o bloccare le richieste Web corrispondenti. Firewall Manager contrassegnerà le risorse interne all'ambito come non conformi se non hanno la mitigazione automatica abilitata o utilizzano un'azione della regola che non corrisponde a quella specificata per la policy. Se si configura la politica per la riparazione automatica, Firewall Manager aggiorna le risorse non conformi secondo necessità.
- Disattiva: se si sceglie di disabilitare la mitigazione automatica, Firewall Manager contrassegnerà le risorse nell'ambito come non conformi se la mitigazione automatica è abilitata. Se si configura la politica per la riparazione automatica, Firewall Manager aggiorna le risorse non conformi secondo necessità.
- Ignora: se scegli di ignorare la mitigazione automatica, Firewall Manager non prenderà in considerazione nessuna delle impostazioni di mitigazione automatica nella politica Shield quando esegue le attività di correzione della policy. Questa impostazione consente di controllare la mitigazione automatica tramite Shield Advanced, senza che tali impostazioni vengano sovrascritte da Firewall Manager. Questa impostazione non si applica alle risorse Classic Load Balancer o Elastic IPs gestite tramite Shield Advanced, poiché Shield Advanced attualmente non supporta la mitigazione automatica L7 per tali risorse.

Sostituisci gli ACL web AWS WAF classici con gli ACL web della versione più recente

La mitigazione automatica degli attacchi DDoS a livello di applicazione funziona solo con gli ACL Web creati utilizzando l'ultima versione di AWS WAF (v2).

Per determinare la versione Web ACL per la tua politica Shield Advanced, consultaDeterminazione della AWS WAF versione utilizzata da una politica Shield Advanced.

Se desideri utilizzare la mitigazione automatica nella tua politica Shield Advanced e la tua politica attualmente utilizza ACL Web AWS WAF classici, puoi creare una nuova politica Shield Advanced per sostituire quella attuale oppure puoi utilizzare le opzioni descritte in questa sezione per sostituire gli ACL Web della versione precedente con i nuovi ACL Web (v2) all'interno della tua politica Shield Advanced corrente. Le nuove politiche creano sempre ACL Web utilizzando la versione più recente di. AWS WAF Se si sostituisce l'intera policy, quando la si elimina, è possibile fare in modo che Firewall Manager elimini anche tutte le ACL Web della versione precedente. Il resto di questa sezione descrive le opzioni per sostituire gli ACL Web all'interno della politica esistente.

Quando modifichi una policy Shield Advanced esistente per CloudFront le risorse Amazon, Firewall Manager può creare automaticamente un nuovo ACL web vuoto AWS WAF (v2) per la policy, in

qualsiasi account pertinente che non disponga già di un ACL web v2. Quando Firewall Manager crea un nuovo ACL web, se la policy ha già un ACL web AWS WAF classico nello stesso account, Firewall Manager configura l'ACL web della nuova versione con la stessa impostazione di azione predefinita dell'ACL web esistente. Se non esiste un ACL web AWS WAF classico, Firewall Manager imposta l'azione predefinita Allow nel nuovo ACL web. Dopo che Firewall Manager ha creato un nuovo ACL Web, è possibile personalizzarlo in base alle esigenze tramite la AWS WAF console.

Quando si sceglie una delle seguenti opzioni di configurazione delle politiche, Firewall Manager crea nuovi ACL Web (v2) per gli account interessati che non li dispongono già:

- Quando abiliti o disabiliti la mitigazione automatica degli attacchi DDoS a livello di applicazione. Questa scelta da sola fa sì che Firewall Manager crei solo i nuovi ACL Web e non sostituisca alcuna associazione ACL Web AWS WAF classica esistente sulle risorse relative all'ambito della policy.
- Quando si sceglie l'azione politica della riparazione automatica e si sceglie l'opzione di sostituire gli ACL web AWS WAF classici con gli ACL web AWS WAF (v2). È possibile scegliere di sostituire gli ACL Web delle versioni precedenti indipendentemente dalle scelte di configurazione per la mitigazione automatica degli attacchi DDoS a livello di applicazione.

  Quando si sceglie l'opzione sostitutiva, Firewall Manager crea gli ACL Web della nuova versione in base alle esigenze e quindi esegue le seguenti operazioni per le risorse relative alla policy:
  - Se una risorsa è associata a un ACL Web da qualsiasi altra politica attiva di Firewall Manager, Firewall Manager lascia solo l'associazione.
  - In tutti gli altri casi, Firewall Manager rimuove qualsiasi associazione con un ACL web AWS WAF classico e associa la risorsa all'ACL web della policy AWS WAF (v2).

Puoi scegliere di fare in modo che Firewall Manager sostituisca gli ACL Web della versione precedente con gli ACL Web della nuova versione quando lo desideri. Se in precedenza hai personalizzato gli ACL web AWS WAF classici della policy, puoi aggiornare gli ACL web della nuova versione con impostazioni comparabili prima di scegliere che Firewall Manager esegua la fase di sostituzione.

È possibile accedere a entrambe le versioni di Web ACL per una policy tramite la console della stessa versione o Classic. AWS WAF AWS WAF

Firewall Manager non elimina gli ACL Web AWS WAF classici sostituiti finché non si elimina la policy stessa. Dopo che gli ACL web AWS WAF classici non sono più utilizzati dalla policy, puoi eliminarli se lo desideri.

Determinazione della AWS WAF versione utilizzata da una politica Shield Advanced

È possibile determinare quale versione della AWS WAF policy Firewall Manager Shield Advanced viene utilizzata esaminando le chiavi dei parametri nella regola AWS Config collegata ai servizi della policy. Se la AWS WAF versione in uso è la più recente, le chiavi dei parametri includono `policyId` e. `webAclArn` Se si tratta della versione precedente, AWS WAF Classic, le chiavi dei parametri includono `webAclId` `eresourceTypes`.

La AWS Config regola elenca solo le chiavi per gli ACL Web attualmente utilizzati dalla policy con le risorse pertinenti.

Per determinare quale versione della AWS WAF policy Firewall Manager Shield Advanced viene utilizzata

1. Recupera l'ID della policy Shield Advanced:

   a. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   b. Nel riquadro di navigazione, scegli Politiche di sicurezza.

   c. Scegli la regione per la politica. Per CloudFront le distribuzioni, questo è`Global`.

   d. Trova la politica che desideri e copia il valore del relativo Policy ID.

      Esempio di ID della politica:`1111111-2222-3333-4444-a55aa5aaa555`.

2. Crea il nome della AWS Config regola aggiungendo l'ID della politica alla stringa`FMManagedShieldConfigRule`.

   Nome di AWS Config regola di esempio:`FMManagedShieldConfigRule1111111-2222-3333-4444-a55aa5aaa555`.

3. Cerca nei parametri della AWS Config regola associata le chiavi denominate `policyId` e`webAclArn`:

   a. Apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.

   b. Nel pannello di navigazione, scegli Regole.

   c. Individua il nome della AWS Config regola della policy del Firewall Manager nell'elenco e selezionalo. Si apre la pagina della regola.

d. In Dettagli della regola, nella sezione Parametri, esamina le chiavi. Se trovi chiavi denominate `policyId` and`webAclArn`, la policy utilizza gli ACL Web creati utilizzando la versione più recente di AWS WAF. Se trovi chiavi denominate `webAclId` and`resourceTypes`, la policy utilizza gli ACL Web creati utilizzando la versione precedente, AWS WAF Classic.

Politiche dei gruppi di sicurezza

Puoi utilizzare le policy AWS Firewall Manager dei gruppi di sicurezza per gestire i gruppi di sicurezza Amazon Virtual Private Cloud per la tua organizzazione in AWS Organizations. È possibile applicare criteri di gruppo di protezione controllati centralmente all'intera organizzazione o a un sottoinsieme selezionato di account e risorse. È inoltre possibile monitorare e gestire i criteri dei gruppi di protezione in uso nell'organizzazione, con criteri di gruppo di protezione di controllo e utilizzo.

Firewall Manager mantiene continuamente le policy e le applica agli account e alle risorse man mano che vengono aggiunte o aggiornate all'interno dell'organizzazione. Per informazioni in merito AWS Organizations, consulta la Guida AWS Organizations per l'utente. Per informazioni sui gruppi di sicurezza di Amazon Virtual Private Cloud, consulta Security Groups for Your VPC nella Amazon VPC User Guide.

È possibile utilizzare le politiche dei gruppi di sicurezza di Firewall Manager per eseguire le seguenti operazioni all'interno AWS dell'organizzazione:

- Applica gruppi di sicurezza comuni agli account e alle risorse specificati.
- Controlla le regole dei gruppi di sicurezza per individuare e correggere le regole non conformi.
- Controlla l'utilizzo dei gruppi di sicurezza per ripulire i gruppi di sicurezza inutilizzati e ridondanti.

Questa sezione illustra come funzionano le policy dei gruppi di sicurezza di Firewall Manager e fornisce indicazioni per il loro utilizzo. Per le procedure per creare le politiche dei gruppi di sicurezza, vedereCreazione di una AWS Firewall Manager politica.

Policy di gruppo di sicurezza comuni

Con una politica comune per i gruppi di sicurezza, Firewall Manager fornisce un'associazione controllata centralmente dei gruppi di sicurezza agli account e alle risorse dell'organizzazione. Specificare dove e come applicare le policy nell'organizzazione.

È possibile applicare politiche comuni per i gruppi di sicurezza ai seguenti tipi di risorse:

- Istanza Amazon Elastic Compute Cloud (Amazon EC2)
- Interfaccia di rete elastica
- Application Load Balancer
- Classic Load Balancer

Per indicazioni sulla creazione di una politica comune per i gruppi di sicurezza tramite la console, consultaCreazione di una policy di gruppo di sicurezza comune.

VPC condivisi

Nelle impostazioni relative all'ambito della policy per una policy di gruppo di sicurezza comune, è possibile scegliere di includere i VPC condivisi. Questa scelta include i VPC di proprietà di un altro account e condivisi con un account rientrante nell'ambito. I VPC che possiedono account rientranti nell'ambito sono sempre inclusi. Per informazioni sui VPC condivisi, consulta Working with shared VPC nella Amazon VPC User Guide.

Le seguenti avvertenze si applicano all'inclusione di VPC condivisi. Queste si aggiungono alle avvertenze generali relative alle politiche dei gruppi di sicurezza riportate all'indirizzo. Limitazioni delle policy di gruppo di sicurezza

- Firewall Manager replica il gruppo di sicurezza primario nei VPC per ogni account interessato. Per un VPC condiviso, Firewall Manager replica il gruppo di sicurezza primario una volta per ogni account interno con cui è condiviso il VPC. Ciò può comportare più repliche in un singolo VPC condiviso.
- Quando crei un nuovo VPC condiviso, non lo vedrai rappresentato nei dettagli delle policy del gruppo di sicurezza Firewall Manager fino a quando non avrai creato almeno una risorsa nel VPC che rientra nell'ambito della policy.
- Quando si disabilitano i VPC condivisi in una policy che aveva abilitato i VPC condivisi, nei VPC condivisi, Firewall Manager elimina i gruppi di sicurezza di replica che non sono associati ad alcuna risorsa. Firewall Manager lascia attivi i restanti gruppi di sicurezza delle repliche, ma smette di gestirli. La rimozione di questi gruppi di sicurezza rimanenti richiede la gestione manuale in ogni istanza VPC condivisa.

Gruppi di sicurezza primari

Per ogni politica di gruppo di sicurezza comune, vengono forniti AWS Firewall Manager uno o più gruppi di sicurezza primari:

- I gruppi di sicurezza primari devono essere creati dall'account amministratore di Firewall Manager e possono risiedere in qualsiasi istanza Amazon VPC dell'account.
- Gestisci i tuoi gruppi di sicurezza principali tramite Amazon Virtual Private Cloud (Amazon VPC) o Amazon Elastic Compute Cloud (Amazon EC2) Elastic Compute Cloud (Amazon EC2). Per informazioni, consulta Working with Security Groups nella Amazon VPC User Guide.
- È possibile nominare uno o più gruppi di sicurezza come primari per una politica di gruppo di sicurezza di Firewall Manager. Per impostazione predefinita, il numero di gruppi di sicurezza consentiti in una policy è uno, ma è possibile inviare una richiesta per aumentarlo. Per informazioni, consulta AWS Firewall Manager quote.

Impostazioni delle regole dei criteri

È possibile scegliere uno o più dei seguenti comportamenti di controllo delle modifiche per i gruppi di sicurezza e le risorse della politica comune dei gruppi di sicurezza:

- Identifica e segnala eventuali modifiche apportate dagli utenti locali alla replica dei gruppi di sicurezza.
- Dissocia gli altri gruppi di sicurezza dalle AWS risorse che rientrano nell'ambito della policy.
- Distribuisci i tag dal gruppo primario ai gruppi di sicurezza di replica.

> **Important**
>
> Firewall Manager non distribuirà i tag di sistema aggiunti dai AWS servizi nei gruppi di sicurezza delle repliche. I tag di sistema iniziano con il prefisso `aws:`. Inoltre, Firewall Manager non aggiornerà i tag dei gruppi di sicurezza esistenti né creerà nuovi gruppi di sicurezza se la policy contiene tag che sono in conflitto con la politica dei tag dell'organizzazione. Per informazioni sulle politiche relative ai tag, consulta le politiche relative ai tag nella Guida AWS Organizations per l'utente.

- Distribuisci i riferimenti ai gruppi di sicurezza dal gruppo primario ai gruppi di sicurezza di replica.

  Ciò consente di stabilire facilmente regole di riferimento comuni ai gruppi di sicurezza su tutte le risorse pertinenti alle istanze associate al VPC del gruppo di sicurezza specificato. Quando abiliti questa opzione, Firewall Manager propaga i riferimenti ai gruppi di sicurezza solo se i gruppi di sicurezza fanno riferimento a gruppi di sicurezza peer in Amazon Virtual Private Cloud. Se i gruppi di sicurezza replicata non fanno correttamente riferimento al gruppo di sicurezza peer, Firewall Manager contrassegna questi gruppi di sicurezza replicati come non conformi. Per informazioni su

come fare riferimento ai gruppi di sicurezza peer in Amazon VPC, consulta Aggiorna i tuoi gruppi di sicurezza per fare riferimento ai gruppi di sicurezza peer nella Amazon VPC Peering Guide.

Se non si abilita questa opzione, Firewall Manager non propaga i riferimenti ai gruppi di sicurezza di replica ai gruppi di sicurezza di replica. Per informazioni sul peering VPC in Amazon VPC, consulta la Amazon VPC Peering Guide.

Creazione e gestione delle politiche

Quando crei una policy comune per i gruppi di sicurezza, Firewall Manager replica i gruppi di sicurezza primari su ogni istanza Amazon VPC nell'ambito della policy e associa i gruppi di sicurezza replicati agli account e alle risorse che rientrano nell'ambito della policy. Quando si modifica un gruppo di sicurezza primario, Firewall Manager propaga la modifica alle repliche.

Quando si elimina un criterio di gruppo di protezione comune, è possibile scegliere se pulire le risorse create dal criterio. Per i gruppi di sicurezza comuni di Firewall Manager, queste risorse sono i gruppi di sicurezza delle repliche. Scegliere l'opzione di pulitura a meno che non si desideri gestire manualmente ogni singola replica dopo l'eliminazione del criterio. Per la maggior parte delle situazioni, scegliere l'opzione di pulizia è l'approccio più semplice.

Come vengono gestite le repliche

I gruppi di sicurezza di replica nelle istanze Amazon VPC sono gestiti come gli altri gruppi di sicurezza Amazon VPC. Per informazioni, consulta Security Groups for Your VPC nella Amazon VPC User Guide.

Policy di gruppo di sicurezza del controllo dei contenuti

Utilizzate le policy dei gruppi di sicurezza per il controllo dei AWS Firewall Manager contenuti per controllare e applicare azioni politiche alle regole in uso nei gruppi di sicurezza dell'organizzazione. Le politiche dei gruppi di sicurezza per il controllo dei contenuti si applicano a tutti i gruppi di sicurezza creati dai clienti e utilizzati nell' AWS organizzazione, in base all'ambito definito nella politica.

Per indicazioni sulla creazione di una policy di gruppo di sicurezza per il controllo dei contenuti tramite la console, consulta. Creazione di una policy di gruppo di sicurezza di controllo del contenuto

Tipo di risorsa ambito criteri

È possibile applicare le policy di gruppo di Content Audit Security ai seguenti tipi di risorse:

- Istanza Amazon Elastic Compute Cloud (Amazon EC2)
- Interfaccia di rete elastica
- Gruppo di sicurezza Amazon VPC

I gruppi di protezione vengono considerati nell'ambito del criterio se sono esplicitamente nell'ambito o se sono associati a risorse nell'ambito.

Opzioni relative alle regole politiche

È possibile utilizzare regole di policy gestite o regole di policy personalizzate per ogni policy di controllo dei contenuti, ma non entrambe.

- Regole di policy gestite: in una policy con regole gestite, è possibile utilizzare elenchi di applicazioni e protocolli per controllare le regole che Firewall Manager controlla e contrassegna come conformi o non conformi. È possibile utilizzare elenchi gestiti da Firewall Manager. È inoltre possibile creare e utilizzare elenchi di applicazioni e protocolli personalizzati. Per informazioni su questi tipi di elenchi e sulle opzioni di gestione degli elenchi personalizzati, vedereElenchi gestiti.
- Regole di policy personalizzate: in una policy con regole di policy personalizzate, si specifica un gruppo di sicurezza esistente come gruppo di sicurezza di controllo per la policy. È possibile utilizzare le regole del gruppo di sicurezza di controllo come modello che definisce le regole che Firewall Manager controlla e contrassegna come conformi o non conformi.

Controlla i gruppi di sicurezza

È necessario creare gruppi di sicurezza di controllo utilizzando l'account amministratore di Firewall Manager, prima di poterli utilizzare nella politica. Puoi gestire i gruppi di sicurezza tramite Amazon Virtual Private Cloud (Amazon VPC) o Amazon Elastic Compute Cloud (Amazon EC2) Elastic Compute Cloud (Amazon EC2). Per informazioni, consulta Working with Security Groups nella Amazon VPC User Guide.

Un gruppo di sicurezza utilizzato per una politica di gruppo di sicurezza di controllo dei contenuti viene utilizzato da Firewall Manager solo come riferimento di confronto per i gruppi di sicurezza che rientrano nell'ambito della politica. Firewall Manager non lo associa ad alcuna risorsa dell'organizzazione.

Il modo in cui si definiscono le regole nel gruppo di sicurezza di controllo dipende dalle scelte effettuate nelle impostazioni delle regole dei criteri:

- Regole dei criteri gestiti: per le impostazioni delle regole dei criteri gestiti, si utilizza un gruppo di sicurezza di controllo per sovrascrivere le altre impostazioni della politica, per consentire o negare esplicitamente regole che altrimenti potrebbero avere un altro risultato di conformità.
  - Se si sceglie di consentire sempre le regole definite nel gruppo di sicurezza di controllo, qualsiasi regola che corrisponde a quella definita nel gruppo di sicurezza di controllo viene considerata conforme alla politica, indipendentemente dalle altre impostazioni della politica.
  - Se si sceglie di negare sempre le regole definite nel gruppo di sicurezza di controllo, qualsiasi regola che corrisponde a quella definita nel gruppo di sicurezza di controllo viene considerata non conforme alla politica, indipendentemente dalle altre impostazioni della politica.
- Regole dei criteri personalizzate: per le impostazioni delle regole dei criteri personalizzate, il gruppo di sicurezza di controllo fornisce l'esempio di ciò che è accettabile o non accettabile nelle regole del gruppo di sicurezza pertinenti:
  - Se si sceglie di consentire l'uso delle regole, tutti i gruppi di sicurezza che rientrano nell'ambito di applicazione devono disporre solo di regole che rientrano nell'intervallo consentito delle regole del gruppo di sicurezza di controllo della policy. In questo caso, le regole del gruppo di sicurezza della policy forniscono l'esempio di cosa è accettabile fare.
  - Se si sceglie di negare l'uso delle regole, tutti i gruppi di sicurezza interessati devono disporre solo di regole che non rientrano nell'intervallo consentito delle regole del gruppo di sicurezza di controllo della policy. In questo caso, il gruppo di sicurezza della policy fornisce l'esempio di cosa non è accettabile fare.

Creazione e gestione delle politiche

Quando si crea un criterio di gruppo di sicurezza di controllo, è necessario disattivare la correzione automatica. La prassi consigliata consiste nell'esaminare gli effetti della creazione dei criteri prima di abilitare la correzione automatica. Dopo aver esaminato gli effetti previsti, è possibile modificare il criterio e abilitare la correzione automatica. Quando la riparazione automatica è abilitata, Firewall Manager aggiorna o rimuove le regole non conformi nei gruppi di sicurezza pertinenti.

Gruppi di protezione interessati da un criterio di gruppo di sicurezza di controllo

Tutti i gruppi di sicurezza dell'organizzazione creati dal cliente sono idonei all'ambito di un criterio di gruppo di sicurezza di controllo.

I gruppi di protezione della replica non vengono creati dal cliente e pertanto non sono idonei a rientrare direttamente nell'ambito di un criterio di gruppo di sicurezza di controllo. Tuttavia, possono essere aggiornati a seguito delle attività di correzione automatica dei criteri. Il gruppo di protezione

principale di un criterio di gruppo di protezione comune è creato dal cliente e può rientrare nell'ambito di un criterio di gruppo di sicurezza di controllo. Se una politica di controllo del gruppo di sicurezza apporta modifiche a un gruppo di sicurezza primario, Firewall Manager propaga automaticamente tali modifiche alle repliche.

Policy di gruppo di sicurezza controllo dell'utilizzo

Utilizza le policy dei gruppi di sicurezza di controllo dell' AWS Firewall Manager utilizzo per monitorare l'organizzazione alla ricerca di gruppi di sicurezza inutilizzati e ridondanti e, facoltativamente, eseguire la pulizia. Quando si abilita la riparazione automatica per questa politica, Firewall Manager esegue le seguenti operazioni:

1. Consolida i gruppi di sicurezza ridondanti, se è stata scelta questa opzione.
2. Rimuove i gruppi di sicurezza inutilizzati, se è stata scelta questa opzione.

È possibile applicare le policy dei gruppi di sicurezza per il controllo dell'utilizzo ai seguenti tipi di risorse:

- Gruppo di sicurezza Amazon VPC

Per indicazioni sulla creazione di una politica di gruppo di sicurezza per il controllo dell'utilizzo utilizzando la console, consultaCreazione di una policy di gruppo di sicurezza di controllo dell'utilizzo.

In che modo Firewall Manager rileva e corregge i gruppi di sicurezza ridondanti

Affinché i gruppi di sicurezza siano considerati ridondanti, devono avere esattamente lo stesso set di regole e trovarsi nella stessa istanza Amazon VPC.

Per correggere un set di gruppi di sicurezza ridondanti, Firewall Manager seleziona uno dei gruppi di sicurezza del set da conservare, quindi lo associa a tutte le risorse associate agli altri gruppi di sicurezza del set. Firewall Manager dissocia quindi gli altri gruppi di sicurezza dalle risorse a cui erano associati, rendendoli inutilizzati.

> **Note**
>
> Se hai scelto di rimuovere anche i gruppi di sicurezza non utilizzati, Firewall Manager esegue questa operazione. Ciò può comportare la rimozione dei gruppi di sicurezza presenti nel set ridondante.

In che modo Firewall Manager rileva e corregge i gruppi di sicurezza inutilizzati

Firewall Manager considera un gruppo di sicurezza inutilizzato se entrambe le seguenti condizioni sono vere:

- Il gruppo di sicurezza non viene utilizzato da nessuna istanza di Amazon EC2 o da un'interfaccia di rete elastica di Amazon EC2.
- Firewall Manager non ha ricevuto un elemento di configurazione relativo entro il numero di minuti specificato nel periodo di tempo della regola dei criteri.

Il periodo di tempo della regola di policy ha un'impostazione predefinita di zero minuti, ma è possibile aumentare il tempo fino a 365 giorni (525.600 minuti), per avere il tempo di associare nuovi gruppi di sicurezza alle risorse.

> **Important**
>
> Se si specifica un numero di minuti diverso dal valore predefinito zero, è necessario abilitare le relazioni indirette in. AWS Config In caso contrario, le politiche del gruppo di sicurezza per il controllo dell'utilizzo non funzioneranno come previsto. Per informazioni sulle relazioni indirette in AWS Config, vedere Relazioni indirette AWS Config nella Guida per gli AWS Config sviluppatori.

Firewall Manager corregge i gruppi di sicurezza inutilizzati eliminandoli dall'account in base alle impostazioni delle regole, se possibile. Se Firewall Manager non è in grado di eliminare un gruppo di sicurezza, lo contrassegna come non conforme alla policy. Firewall Manager non può eliminare un gruppo di sicurezza a cui fa riferimento un altro gruppo di sicurezza.

La tempistica della riparazione varia a seconda che si utilizzi l'impostazione del periodo di tempo predefinita o un'impostazione personalizzata:

- Periodo di tempo impostato su zero, l'impostazione predefinita: con questa impostazione, un gruppo di sicurezza viene considerato inutilizzato non appena non viene utilizzato da un'istanza Amazon EC2 o da un'interfaccia di rete elastica.

  Per questa impostazione del periodo di tempo zero, Firewall Manager corregge immediatamente il gruppo di sicurezza.

- Periodo di tempo maggiore di zero: con questa impostazione, un gruppo di sicurezza viene considerato inutilizzato quando non viene utilizzato da un'istanza Amazon EC2 o da un'interfaccia di rete elastica e Firewall Manager non ha ricevuto un elemento di configurazione per esso entro il numero di minuti specificato.

  Per l'impostazione del periodo di tempo diverso da zero, Firewall Manager corregge il gruppo di sicurezza dopo che è rimasto nello stato inutilizzato per 24 ore.

Specificazioni account predefinite

Quando si crea una policy di gruppo di sicurezza per il controllo dell'utilizzo tramite la console, Firewall Manager sceglie automaticamente Escludi gli account specificati e includi tutti gli altri. Il servizio inserisce quindi l'account amministratore di Firewall Manager nell'elenco da escludere. Questo è l'approccio consigliato e consente di gestire manualmente i gruppi di sicurezza che appartengono all'account amministratore di Firewall Manager.

Procedure consigliate per policy di gruppo di sicurezza

In questa sezione sono elencati i suggerimenti per la gestione dei gruppi di sicurezza mediante AWS Firewall Manager:

Escludere l'account amministratore di Firewall Manager

Quando si imposta l'ambito della politica, si esclude l'account amministratore di Firewall Manager. Quando si crea un criterio di gruppo di protezione controllo dell'utilizzo tramite la console, questa è l'opzione predefinita.

Avvio con la correzione automatica disabilitata

Per i criteri del gruppo di protezione del controllo del contenuto o dell'utilizzo, iniziare con la correzione automatica disabilitata. Esaminare le informazioni dettagliate sui criteri per determinare gli effetti che la correzione automatica avrebbe avuto. Quando si è certi che le modifiche sono ciò che si desidera, modificare il criterio per abilitare la correzione automatica.

Evitare conflitti se si utilizzano anche origini esterne per gestire i gruppi di sicurezza

Se si utilizza uno strumento o un servizio diverso da Firewall Manager per gestire i gruppi di sicurezza, fare attenzione a evitare conflitti tra le impostazioni in Firewall Manager e le impostazioni nella fonte esterna. Se si utilizzano la correzione automatica e il conflitto di impostazioni, è possibile creare un ciclo di correzione in conflitto che consuma risorse su entrambi i lati.

Ad esempio, supponiamo di configurare un altro servizio per gestire un gruppo di sicurezza per un set di AWS risorse e di configurare una politica di Firewall Manager per mantenere un gruppo di sicurezza diverso per alcune o tutte le stesse risorse. Se si configura uno dei due lati per non consentire l'associazione di altri gruppi di sicurezza alle risorse nell'ambito, tale lato rimuoverà l'associazione dei gruppi di sicurezza mantenuta dall'altro lato. Se entrambi i lati sono configurati in questo modo, si può finire con un ciclo di disassociazioni e associazioni in conflitto.

Inoltre, supponiamo di creare una politica di controllo di Firewall Manager per applicare una configurazione del gruppo di sicurezza in conflitto con la configurazione del gruppo di sicurezza dell'altro servizio. La correzione applicata dalla politica di controllo di Firewall Manager può aggiornare o eliminare quel gruppo di sicurezza, rendendolo non conforme per l'altro servizio. Se l'altro servizio è configurato per monitorare e risolvere automaticamente eventuali problemi rilevati, ricreerà o aggiornerà il gruppo di sicurezza, rendendolo nuovamente non conforme alla politica di controllo di Firewall Manager. Se la politica di controllo di Firewall Manager è configurata con la riparazione automatica, aggiornerà o eliminerà nuovamente il gruppo di sicurezza esterno e così via.

Per evitare conflitti come questi, create configurazioni che si escludano a vicenda, tra Firewall Manager e qualsiasi fonte esterna.

È possibile utilizzare i tag per escludere i gruppi di sicurezza esterni dalla riparazione automatica mediante le politiche di Firewall Manager. A tale scopo, aggiungere uno o più tag ai gruppi di sicurezza o ad altre risorse gestite dall'origine esterna. Quindi, quando definisci l'ambito della policy di Firewall Manager, nelle specifiche delle risorse, escludi le risorse che hanno il tag o i tag che hai aggiunto.

Analogamente, nello strumento o servizio esterno, escludi i gruppi di sicurezza gestiti da Firewall Manager da qualsiasi attività di gestione o controllo. Non importate le risorse di Firewall Manager o utilizzate i tag specifici di Firewall Manager per escluderle dalla gestione esterna.

Procedure ottimali per l'utilizzo, il controllo delle politiche di sicurezza dei gruppi.

Segui queste linee guida quando utilizzi le politiche dei gruppi di sicurezza per il controllo dell'utilizzo.

- Evita di apportare più modifiche allo stato di associazione di un gruppo di sicurezza in un breve lasso di tempo, ad esempio entro una finestra di 15 minuti. In questo modo, Firewall Manager potrebbe perdere alcuni o tutti gli eventi corrispondenti. Ad esempio, non associare e dissociare rapidamente un gruppo di sicurezza da un'interfaccia di rete elastica.
- Non utilizzate il registratore di AWS Config configurazione per verificare l'utilizzo delle politiche dei gruppi di sicurezza. Non è necessario e il suo utilizzo comporta costi aggiuntivi AWS Config .

Limitazioni delle policy di gruppo di sicurezza

Questa sezione elenca le limitazioni all'utilizzo delle politiche dei gruppi AWS Firewall Manager di sicurezza:

- L'aggiornamento dei gruppi di sicurezza per le interfacce di rete elastiche di Amazon EC2 create utilizzando il tipo di servizio Fargate non è supportato. Tuttavia, puoi aggiornare i gruppi di sicurezza per le interfacce di rete elastiche di Amazon ECS con il tipo di servizio Amazon EC2.
- Firewall Manager non supporta i gruppi di sicurezza per le interfacce di rete elastiche di Amazon EC2 create da Amazon Relational Database Service.
- L'aggiornamento delle interfacce di rete elastiche di Amazon ECS è possibile solo per i servizi Amazon ECS che utilizzano il controller di distribuzione Rolling Update (Amazon ECS). Per altri controller di distribuzione Amazon ECS come CODE_DEPLOY o controller esterni, Firewall Manager attualmente non è in grado di aggiornare le interfacce di rete elastiche.
- Con i gruppi di sicurezza per le interfacce di rete elastiche di Amazon EC2, le modifiche a un gruppo di sicurezza non sono immediatamente visibili a Firewall Manager. Firewall Manager di solito rileva le modifiche entro diverse ore, ma il rilevamento può essere ritardato fino a sei ore.
- Firewall Manager non supporta l'aggiornamento dei gruppi di sicurezza nelle interfacce di rete elastiche per Network Load Balancer.
- Nelle politiche comuni dei gruppi di sicurezza, se un VPC condiviso viene successivamente annullato con un account, Firewall Manager non eliminerà i gruppi di sicurezza di replica presenti nell'account.
- Con le policy dei gruppi di sicurezza di usage audit, se si creano più policy con un'impostazione personalizzata del tempo di ritardo che hanno tutte lo stesso ambito, la prima policy con i risultati di conformità sarà la politica che riporta i risultati.

Casi d'uso delle policy di gruppo di sicurezza

Puoi utilizzare politiche AWS Firewall Manager comuni dei gruppi di sicurezza per automatizzare la configurazione del firewall host per la comunicazione tra istanze Amazon VPC. Questa sezione elenca le architetture standard di Amazon VPC e descrive come proteggerle utilizzando le politiche comuni dei gruppi di sicurezza di Firewall Manager. Queste policy dei gruppi di sicurezza possono aiutarti ad applicare un set unificato di regole per selezionare le risorse in diversi account ed evitare configurazioni per account in Amazon Elastic Compute Cloud e Amazon VPC.

Con le politiche comuni dei gruppi di sicurezza di Firewall Manager, puoi etichettare solo le interfacce di rete elastiche EC2 necessarie per la comunicazione con le istanze in un altro Amazon VPC. Le altre istanze nello stesso Amazon VPC sono quindi più sicure e isolate.

Caso d'uso: monitoraggio e controllo delle richieste agli Application Load Balancer e ai Classic Load Balancer

È possibile utilizzare una politica di gruppo di sicurezza comune di Firewall Manager per definire le richieste che i sistemi di bilanciamento del carico interessati devono soddisfare. È possibile configurarlo tramite la console Firewall Manager. Solo le richieste conformi alle regole in entrata del gruppo di sicurezza possono raggiungere i sistemi di bilanciamento del carico, che distribuiranno solo le richieste che soddisfano le regole in uscita.

Caso d'uso: Amazon VPC pubblico e accessibile da Internet

Puoi utilizzare una policy di gruppo di sicurezza comune di Firewall Manager per proteggere un Amazon VPC pubblico, ad esempio per consentire solo la porta in entrata 443. Ciò equivale a consentire solo il traffico HTTPS in ingresso per un VPC pubblico. È possibile etichettare le risorse pubbliche all'interno del VPC (ad esempio, come «PublicVPC») e quindi impostare l'ambito della policy di Firewall Manager solo sulle risorse con quel tag. Firewall Manager applica automaticamente la policy a tali risorse.

Caso d'uso: istanze Amazon VPC pubbliche e private

Puoi utilizzare la stessa politica comune dei gruppi di sicurezza per le risorse pubbliche consigliata nel caso d'uso precedente per le istanze Amazon VPC pubbliche accessibili da Internet. È possibile utilizzare un secondo criterio comune di gruppo di protezione per limitare la comunicazione tra le risorse pubbliche e quelle private. Etichetta le risorse nelle istanze Amazon VPC pubbliche e private con qualcosa come "PublicPrivate" per applicare loro la seconda policy. Puoi utilizzare una terza policy per definire la comunicazione consentita tra le risorse private e altre istanze Amazon VPC aziendali o private. Per questo criterio, è possibile utilizzare un altro tag identificativo sulle risorse private.

Caso d'uso: istanze Amazon VPC Hub and spoke

Puoi utilizzare una policy di gruppo di sicurezza comune per definire le comunicazioni tra l'istanza Amazon VPC hub e le istanze Amazon VPC spoke. Puoi utilizzare una seconda policy per definire la comunicazione da ogni istanza Amazon VPC spoke all'istanza Amazon VPC hub.

Caso d'uso: interfaccia di rete predefinita per le istanze Amazon EC2

È possibile utilizzare un criterio di gruppo di protezione comune per consentire solo le comunicazioni standard, ad esempio i servizi di aggiornamento SSH e Patch/OS interni, e per non consentire altre comunicazioni non sicure.

Caso d'uso: identifica le risorse con autorizzazioni aperte

È possibile utilizzare un criterio di gruppo di sicurezza di controllo per identificare tutte le risorse all'interno dell'organizzazione che dispongono dell'autorizzazione per comunicare con gli indirizzi IP pubblici o con indirizzi IP appartenenti a fornitori di terze parti.

AWS Network Firewall politiche

Puoi utilizzare le policy AWS Firewall Manager Network Firewall per gestire i AWS Network Firewall firewall per i tuoi VPC Amazon Virtual Private Cloud in tutta l'organizzazione in. AWS Organizations Puoi applicare firewall controllati centralmente all'intera organizzazione o a un sottoinsieme selezionato di account e VPC.

Network Firewall fornisce protezioni di filtraggio del traffico di rete per le sottoreti pubbliche nei tuoi VPC. Firewall Manager crea e gestisce i firewall in base al tipo di gestione del firewall definito dalla policy. Firewall Manager fornisce i seguenti modelli di gestione del firewall:

- Distribuito: per ogni account e VPC che rientra nell'ambito delle policy, Firewall Manager crea un firewall Network Firewall e distribuisce gli endpoint del firewall nelle sottoreti VPC, per filtrare il traffico di rete.
- Centralizzato: Firewall Manager crea un unico firewall Network Firewall in un unico Amazon VPC.
- Importa firewall esistenti: Firewall Manager importa i firewall esistenti per la gestione in un'unica politica di Firewall Manager. Puoi applicare regole aggiuntive ai firewall importati gestiti dalla tua politica per garantire che i firewall soddisfino gli standard di sicurezza.

> **Note**
>
> Le politiche Firewall di rete di Firewall Manager sono politiche di Firewall Manager che utilizzi per gestire le protezioni dei firewall di rete per i tuoi VPC all'interno dell'organizzazione.
> Le protezioni Network Firewall sono specificate nelle risorse del servizio Network Firewall denominate politiche firewall.

Per informazioni sull'utilizzo di Network Firewall, consulta la Guida per AWS Network Firewall gli sviluppatori.

Le sezioni seguenti illustrano i requisiti per l'utilizzo delle politiche Firewall di Firewall Manager Network e ne descrivono il funzionamento. Per la procedura di creazione della policy, vedereCreazione di una AWS Firewall Manager politica per AWS Network Firewall.

È necessario abilitare la condivisione delle risorse

Una policy Network Firewall condivide i gruppi di regole del Network Firewall tra gli account dell'organizzazione. Affinché funzioni, è necessario che la condivisione delle risorse sia abilitata per AWS Organizations. Per informazioni su come abilitare la condivisione delle risorse, vedereCondivisione delle risorse per le politiche Network Firewall e DNS Firewall.

È necessario che i gruppi di regole del Network Firewall siano definiti

Quando si specifica una nuova policy Network Firewall, la si definisce nello stesso modo in cui si definisce quando si utilizza AWS Network Firewall direttamente. È possibile specificare i gruppi di regole stateless da aggiungere, le azioni stateless predefinite e i gruppi di regole stateless. I gruppi di regole devono già esistere nell'account amministratore di Firewall Manager per poterli includere nella policy. Per informazioni sulla creazione di gruppi di regole Network Firewall, vedere gruppi di AWS Network Firewall regole.

Come Firewall Manager crea endpoint firewall

Il tipo di gestione del firewall nella politica determina il modo in cui Firewall Manager crea i firewall. La tua policy può creare firewall distribuiti, un firewall centralizzato oppure puoi importare firewall esistenti:

- Distribuito: con il modello di distribuzione distribuito, Firewall Manager crea endpoint per ogni VPC che rientra nell'ambito delle policy. È possibile personalizzare la posizione degli endpoint specificando in quali zone di disponibilità creare gli endpoint firewall oppure Firewall Manager può creare automaticamente gli endpoint nelle zone di disponibilità con sottoreti pubbliche. Se si scelgono manualmente le zone di disponibilità, è possibile limitare l'insieme di CIDR consentiti per zona di disponibilità. Se decidi di consentire a Firewall Manager di creare automaticamente gli endpoint, devi anche specificare se il servizio creerà un singolo endpoint o più endpoint firewall all'interno dei tuoi VPC.
  - Per più endpoint firewall, Firewall Manager implementa un endpoint firewall in ogni zona di disponibilità in cui è presente una sottorete con un gateway Internet o una route di endpoint

firewall creata da Firewall Manager nella tabella di routing. Questa è l'opzione predefinita per una politica Network Firewall.

- Per un singolo endpoint firewall, Firewall Manager implementa un endpoint firewall in una singola zona di disponibilità in qualsiasi sottorete dotata di un percorso gateway Internet. Con questa opzione, il traffico in altre zone deve attraversare i confini delle zone per essere filtrato dal firewall.

> **Note**
>
> Per entrambe queste opzioni, deve esserci una sottorete associata a una tabella di route contenente una route IPv4/PrefixList. Firewall Manager non verifica la presenza di altre risorse.

- Centralizzato: con il modello di distribuzione centralizzato, Firewall Manager crea uno o più endpoint firewall all'interno di un VPC di ispezione. Un VPC di ispezione è un VPC centrale in cui Firewall Manager avvia gli endpoint. Quando si utilizza il modello di distribuzione centralizzato, si specifica anche in quali zone di disponibilità creare gli endpoint del firewall. Non puoi modificare il VPC di ispezione dopo aver creato la tua politica. Per utilizzare un VPC di ispezione diverso, è necessario creare una nuova politica.
- Importa firewall esistenti: quando importi firewall esistenti, scegli i firewall da gestire nella tua politica aggiungendo uno o più set di risorse alla tua politica. Un set di risorse è una raccolta di risorse, in questo caso firewall esistenti in Network Firewall, gestite da un account dell'organizzazione. Prima di utilizzare i set di risorse nella politica, è necessario innanzitutto creare un set di risorse. Per informazioni sui set di risorse di Firewall Manager, vedereUtilizzo dei set di risorse in Firewall Manager.

  Tieni presente le seguenti considerazioni quando lavori con firewall importati:

  - Se un firewall importato diventa non conforme, Firewall Manager tenterà di risolvere automaticamente la violazione, tranne nelle seguenti circostanze:
    - Se c'è una discrepanza tra le azioni predefinite stateful o stateless della policy Firewall Manager e Network Firewall.
    - Se un gruppo di regole nella politica firewall di un firewall importato ha la stessa priorità di un gruppo di regole nella politica di Firewall Manager.
    - Se un firewall importato utilizza una politica firewall associata a un firewall che non fa parte del set di risorse della policy. Ciò può accadere perché un firewall può avere esattamente una politica firewall, ma una singola politica firewall può essere associata a più firewall.

  - Se a un gruppo di regole preesistente appartenente alla politica firewall di un firewall importato, specificata anche nella politica di Firewall Manager, viene assegnata una priorità diversa.
- Se si abilita la pulizia delle risorse nella politica, Firewall Manager rimuove i gruppi di regole inclusi nella politica di importazione FMS dai firewall nell'ambito del set di risorse.
- I firewall gestiti da Firewall Manager che importano un tipo di gestione firewall esistente possono essere gestiti solo da una policy alla volta. Se lo stesso set di risorse viene aggiunto a più policy firewall di rete di importazione, i firewall del set di risorse verranno gestiti in base alla prima policy a cui è stato aggiunto il set di risorse e ignorati dalla seconda politica.
- Firewall Manager attualmente non trasmette in streaming le configurazioni dei criteri di eccezione. Per informazioni sulle politiche relative alle eccezioni di flusso, consulta la sezione Politica delle eccezioni di flusso nella Guida per gli AWS Network Firewall sviluppatori.

Se si modifica l'elenco delle zone di disponibilità per le politiche che utilizzano la gestione distribuita o centralizzata del firewall, Firewall Manager tenterà di ripulire tutti gli endpoint creati in passato, ma che attualmente non rientrano nell'ambito delle policy. Firewall Manager rimuoverà l'endpoint solo se non ci sono route della tabella di routing che fanno riferimento all'endpoint fuori ambito. Se Firewall Manager rileva di non essere in grado di eliminare questi endpoint, contrassegnerà la sottorete del firewall come non conforme e continuerà a tentare di rimuovere l'endpoint fino a quando l'eliminazione non sarà sicura.

In che modo Firewall Manager gestisce le sottoreti del firewall

Le sottoreti firewall sono le sottoreti VPC create da Firewall Manager per gli endpoint firewall che filtrano il traffico di rete. Ogni endpoint firewall deve essere distribuito in una sottorete VPC dedicata. Firewall Manager crea almeno una sottorete firewall in ogni VPC che rientra nell'ambito della policy.

Per le politiche che utilizzano il modello di distribuzione distribuito con configurazione automatica degli endpoint, Firewall Manager crea solo sottoreti firewall nelle zone di disponibilità che dispongono di una sottorete con un percorso gateway Internet o una sottorete con un percorso verso gli endpoint firewall creati da Firewall Manager per la loro politica. Per ulteriori informazioni, consulta VPC e sottoreti nella Guida per l'utente di Amazon VPC.

Per le policy che utilizzano il modello distribuito o centralizzato in cui si specifica in quali zone di disponibilità Firewall Manager crea gli endpoint del firewall, Firewall Manager crea un endpoint in quelle zone di disponibilità specifiche indipendentemente dalla presenza di altre risorse nella zona di disponibilità.

Quando si definisce per la prima volta una politica di Network Firewall, si specifica in che modo Firewall Manager gestisce le sottoreti firewall in ciascuno dei VPC inclusi nell'ambito. Non è possibile modificare questa scelta in un secondo momento.

Per le politiche che utilizzano il modello di distribuzione distribuito con configurazione automatica degli endpoint, puoi scegliere tra le seguenti opzioni:

- Implementa una sottorete firewall per ogni zona di disponibilità con sottoreti pubbliche. Questo è il comportamento che segue di default. Ciò garantisce un'elevata disponibilità delle protezioni di filtraggio del traffico.
- Implementa una singola sottorete del firewall in un'unica zona di disponibilità. Con questa scelta, Firewall Manager identifica una zona del VPC con il maggior numero di sottoreti pubbliche e vi crea la sottorete firewall. L'endpoint firewall singolo filtra tutto il traffico di rete per il VPC. Ciò può ridurre i costi del firewall, ma non è altamente disponibile e richiede che il traffico proveniente da altre zone attraversi i confini delle zone per poter essere filtrato.

Per le politiche che utilizzano il modello di distribuzione distribuito con configurazione personalizzata degli endpoint o il modello di distribuzione centralizzato, Firewall Manager crea le sottoreti nelle zone di disponibilità specificate che rientrano nell'ambito della policy.

È possibile fornire blocchi VPC CIDR a Firewall Manager da utilizzare per le sottoreti del firewall oppure lasciare la scelta degli indirizzi degli endpoint del firewall a Firewall Manager.

- Se non fornisci blocchi CIDR, Firewall Manager richiede ai tuoi VPC gli indirizzi IP disponibili da utilizzare.
- Se fornisci un elenco di blocchi CIDR, Firewall Manager cerca nuove sottoreti solo nei blocchi CIDR che fornisci. È necessario utilizzare blocchi CIDR /28. Per ogni sottorete firewall creata da Firewall Manager, analizza l'elenco di blocchi CIDR e utilizza la prima che ritiene applicabile alla zona di disponibilità e al VPC e che presenta indirizzi disponibili. Se Firewall Manager non è in grado di trovare spazio aperto nel VPC (con o senza la restrizione), il servizio non creerà un firewall nel VPC.

Se Firewall Manager non è in grado di creare una sottorete firewall richiesta in una zona di disponibilità, contrassegna la sottorete come non conforme alla policy. Mentre la zona si trova in questo stato, il traffico destinato alla zona deve attraversare i confini della zona per essere filtrato da un endpoint in un'altra zona. Questo è simile allo scenario di sottorete a firewall singolo.

Come Firewall Manager gestisce le risorse del Network Firewall

Quando si definisce la politica in Firewall Manager, si fornisce il comportamento di filtraggio del traffico di rete di una politica AWS Network Firewall firewall standard. Si aggiungono gruppi di regole di Network Firewall stateless e stateful e si specificano azioni predefinite per i pacchetti che non soddisfano alcuna regola stateless. Per informazioni sull'utilizzo delle politiche del firewall in AWS Network Firewall, consulta le politiche del firewall.AWS Network Firewall

Per le policy distribuite e centralizzate, quando si salva la policy Network Firewall, Firewall Manager crea una policy firewall e firewall in ogni VPC che rientra nell'ambito della policy. Firewall Manager assegna un nome a queste risorse Network Firewall concatenando i seguenti valori:

- Una stringa fissa, `FMManagedNetworkFirewall` oppure`FMManagedNetworkFirewallPolicy`, a seconda del tipo di risorsa.
- Nome della policy di Firewall Manager. Questo è il nome che si assegna quando si crea la policy.
- ID della politica di Firewall Manager. Questo è l'ID della AWS risorsa per la policy Firewall Manager.
- ID Amazon VPC. Questo è l'ID di AWS risorsa per il VPC in cui Firewall Manager crea il firewall e la policy del firewall.

Di seguito viene illustrato un esempio di nome per un firewall gestito da Firewall Manager:

```
FMManagedNetworkFirewallEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

Di seguito viene illustrato un esempio di nome della politica del firewall:

```
FMManagedNetworkFirewallPolicyEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

Dopo aver creato la policy, gli account dei membri nei VPC non possono sovrascrivere le impostazioni delle policy firewall o i gruppi di regole, ma possono aggiungere gruppi di regole alla policy firewall creata da Firewall Manager.

In che modo Firewall Manager gestisce e monitora le tabelle di routing VPC per la tua policy

> **Note**
>
> La gestione delle tabelle di routing non è attualmente supportata per le policy che utilizzano il modello di distribuzione centralizzato.

Quando Firewall Manager crea gli endpoint firewall, crea anche le relative tabelle di routing VPC. Tuttavia, Firewall Manager non gestisce le tabelle di routing VPC. È necessario configurare le tabelle di routing VPC per indirizzare il traffico di rete verso gli endpoint firewall creati da Firewall Manager. Utilizzando i miglioramenti del routing di ingresso di Amazon VPC, modifica le tabelle di routing per instradare il traffico attraverso i nuovi endpoint del firewall. Le modifiche devono inserire gli endpoint del firewall tra le sottoreti che desideri proteggere e le ubicazioni esterne. L'esatto routing da eseguire dipende dall'architettura e dai suoi componenti.

Attualmente, Firewall Manager consente il monitoraggio dei percorsi della tabella di routing VPC per qualsiasi traffico destinato al gateway Internet, ovvero aggirando il firewall. Firewall Manager non supporta altri gateway di destinazione come i gateway NAT.

Per informazioni sulla gestione delle tabelle di routing per il tuo VPC, consulta Managing route tables for your VPC nella Amazon Virtual Private Cloud User Guide. Per informazioni sulla gestione delle tabelle di routing per Network Firewall, consulta la sezione Configurazioni delle tabelle di routing AWS Network Firewall nella AWS Network Firewall Developer Guide.

Quando abiliti il monitoraggio di una policy, Firewall Manager monitora continuamente le configurazioni degli instradamenti VPC e ti avvisa del traffico che aggira l'ispezione del firewall per quel VPC. Se una sottorete ha una route degli endpoint firewall, Firewall Manager cerca le seguenti route:

- Percorsi per inviare traffico all'endpoint Network Firewall.
- Percorsi per inoltrare il traffico dall'endpoint Network Firewall al gateway Internet.
- Percorsi in entrata dal gateway Internet all'endpoint Network Firewall.
- Percorsi dalla sottorete del firewall.

Se una sottorete ha una route Network Firewall ma il routing è asimmetrico in Network Firewall e nella tabella di routing del gateway Internet, Firewall Manager segnala la sottorete come non conforme. Firewall Manager rileva anche le route verso il gateway Internet nella tabella di routing del firewall creata da Firewall Manager, nonché nella tabella di routing per la sottorete, e le segnala come non conformi. Anche le route aggiuntive nella tabella di routing della sottorete Network Firewall e nella tabella di routing del gateway Internet vengono segnalate come non conformi. A seconda del tipo di violazione, Firewall Manager suggerisce azioni correttive per rendere conforme la configurazione del percorso. Firewall Manager non offre suggerimenti in tutti i casi. Ad esempio, se la sottorete del cliente ha un endpoint firewall creato all'esterno di Firewall Manager, Firewall Manager non suggerisce azioni correttive.

Per impostazione predefinita, Firewall Manager contrassegna come non conforme tutto il traffico che attraversa il confine della zona di disponibilità per l'ispezione. Tuttavia, se scegli di creare automaticamente un singolo endpoint nel tuo VPC, Firewall Manager non contrassegnerà il traffico che attraversa il confine della zona di disponibilità come non conforme.

Per le policy che utilizzano modelli di distribuzione distribuiti con configurazione personalizzata degli endpoint, è possibile scegliere se il traffico che attraversa il confine della zona di disponibilità da una zona di disponibilità senza un endpoint firewall sia contrassegnato come conforme o non conforme.

> **Note**
>
> - Firewall Manager non suggerisce azioni correttive per route non IPv4, come IPv6 e route con elenco di prefissi.
> - Il rilevamento delle chiamate effettuate utilizzando la chiamata `DisassociateRouteTable` API può richiedere fino a 12 ore.
> - Firewall Manager crea una tabella di routing del Network Firewall per una sottorete che contiene gli endpoint del firewall. Firewall Manager presuppone che questa tabella di routing contenga solo gateway Internet validi e route predefinite VPC. Tutte le route aggiuntive o non valide in questa tabella di routing sono considerate non conformi.

Quando si configura la politica di Firewall Manager, se si sceglie la modalità Monitor, Firewall Manager fornisce dettagli sulla violazione delle risorse e sulla correzione delle risorse. È possibile utilizzare queste azioni correttive suggerite per risolvere i problemi di routing nelle tabelle di routing. Se scegli la modalità Off, Firewall Manager non monitora per te il contenuto della tabella di routing. Con questa opzione, gestisci da solo le tabelle di routing in VPC. Per ulteriori informazioni su queste violazioni delle risorse, consultaVisualizzazione delle informazioni sulla conformità per una AWS Firewall Manager politica.

> **Warning**
>
> Se scegli Monitor nella configurazione del AWS Network Firewall percorso durante la creazione della tua policy, non puoi disattivarla per quella policy. Tuttavia, se scegli Off, puoi abilitarla in un secondo momento.

Configurazione della registrazione per una politica AWS Network Firewall

È possibile abilitare la registrazione centralizzata per le politiche del Network Firewall per ottenere informazioni dettagliate sul traffico all'interno dell'organizzazione. È possibile selezionare la registrazione del flusso per acquisire il flusso di traffico di rete o la registrazione degli avvisi per segnalare il traffico che corrisponde a una regola con l'azione impostata su o. `DROP` `ALERT` Per ulteriori informazioni sulla AWS Network Firewall registrazione, consulta la sezione Registrazione del traffico di rete dalla AWS Network Firewall Guida per gli sviluppatori.AWS Network Firewall

Invii i log dai firewall Network Firewall della tua politica a un bucket Amazon S3. Dopo aver abilitato la registrazione, AWS Network Firewall fornisce i log per ogni Network Firewall configurato aggiornando le impostazioni del firewall per inviare i log ai bucket Amazon S3 selezionati con il prefisso riservato,. AWS Firewall Manager `<policy-name>-<policy-id>`

> **Note**
>
> Questo prefisso viene utilizzato da Firewall Manager per determinare se una configurazione di registrazione è stata aggiunta da Firewall Manager o se è stata aggiunta dal proprietario dell'account. Se il proprietario dell'account tenta di utilizzare il prefisso riservato per la propria registrazione personalizzata, questo viene sovrascritto dalla configurazione di registrazione nella politica di Firewall Manager.

Per ulteriori informazioni su come creare un bucket Amazon S3 e rivedere i log archiviati, consulta Cos'è Amazon S3? nella Guida per l'utente di Amazon Simple Storage Service.

Per abilitare la registrazione devi soddisfare i seguenti requisiti:

- L'Amazon S3 specificato nella policy di Firewall Manager deve esistere.
- Bisogna possedere le seguenti autorizzazioni:
  - `logs:CreateLogDelivery`
  - `s3:GetBucketPolicy`
  - `s3:PutBucketPolicy`
- Se il bucket Amazon S3 che è la tua destinazione di registrazione utilizza la crittografia lato server con chiavi archiviate in AWS Key Management Service, devi aggiungere la seguente policy alla tua chiave AWS KMS gestita dal cliente per consentire a Firewall Manager di accedere al tuo gruppo di log Logs: CloudWatch

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt*",
        "kms:Decrypt*",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:Describe*"
    ],
    "Resource": "*"
}
```

Tieni presente che solo i bucket nell'account amministratore di Firewall Manager possono essere utilizzati per la registrazione AWS Network Firewall centralizzata.

Quando si abilita la registrazione centralizzata su una politica Network Firewall, Firewall Manager esegue le seguenti azioni sull'account:

- Firewall Manager aggiorna le autorizzazioni su bucket S3 selezionati per consentire la consegna dei log.
- Firewall Manager crea directory nel bucket S3 per ogni account membro nell'ambito della policy. I log di ogni account sono disponibili all'indirizzo. `<bucket-name>/<policy-name>-<policy-id>/AWSLogs/<account-id>`

Per abilitare la registrazione per una politica Network Firewall

1. Crea un bucket Amazon S3 utilizzando il tuo account amministratore di Firewall Manager. Per ulteriori informazioni, consulta Creare un bucket nella Guida per l'utente di Amazon Simple Storage Service.
2. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

> **Note**
>
> Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

3. Nel riquadro di navigazione, scegli Politiche di sicurezza.
4. Scegli la politica Network Firewall per la quale desideri abilitare la registrazione. Per ulteriori informazioni sulla AWS Network Firewall registrazione, consulta la sezione Registrazione del traffico di rete dalla Guida per AWS Network Firewall gli AWS Network Firewall sviluppatori.
5. Nella scheda Dettagli della politica, nella sezione Regole della politica, scegli Modifica.
6. Per abilitare e aggregare i log, scegli una o più opzioni in Configurazione della registrazione:
   - Abilita e aggrega i log di flusso
   - Abilita e aggrega i registri degli avvisi
7. Scegli il bucket Amazon S3 in cui desideri che vengano consegnati i log. Devi scegliere un bucket per ogni tipo di log che abiliti. Puoi usare lo stesso bucket per entrambi i tipi di log.
8. (Facoltativo) Se desideri che la registrazione personalizzata creata dall'account membro venga sostituita con la configurazione di registrazione della politica, scegli Sostituisci la configurazione di registrazione esistente.
9. Seleziona Successivo.
10. Controlla le impostazioni, quindi scegli Salva per salvare le modifiche alla politica.

Per disabilitare la registrazione per una politica Network Firewall

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

> **Note**
>
> Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegli Politiche di sicurezza.

3. Scegli la politica Network Firewall per la quale desideri disabilitare la registrazione.
4. Nella scheda Dettagli della politica, nella sezione Regole della politica, scegli Modifica.
5. In Registrazione dello stato di configurazione, deseleziona Abilita e aggrega i log di flusso e Abilita e aggrega i log degli avvisi, se selezionati.
6. Seleziona Successivo.
7. Controlla le impostazioni, quindi scegli Salva per salvare le modifiche alla politica.

Politiche del firewall DNS di Amazon Route 53 Resolver

Puoi utilizzare le policy AWS Firewall Manager DNS Firewall per gestire le associazioni tra i gruppi di regole di Amazon Route 53 Resolver DNS Firewall e i tuoi VPC Amazon Virtual Private Cloud in tutta l'organizzazione in. AWS Organizations Puoi applicare gruppi di regole controllati centralmente all'intera organizzazione o a un sottoinsieme selezionato di account e VPC.

DNS Firewall fornisce il filtraggio e la regolazione del traffico DNS in uscita per i tuoi VPC. Crei raccolte riutilizzabili di regole di filtraggio nei gruppi di regole del firewall DNS e associ i gruppi di regole ai tuoi VPC. Quando si applica la politica di Firewall Manager, per ogni account e VPC che rientra nell'ambito della policy, Firewall Manager crea un'associazione tra ogni gruppo di regole DNS Firewall nella policy e ogni VPC che rientra nell'ambito della policy, utilizzando le impostazioni di priorità di associazione specificate nella policy di Firewall Manager.

Per informazioni sull'uso di DNS Firewall, consulta Amazon Route 53 Resolver DNS Firewall nella Amazon Route 53 Developer Guide.

Le seguenti sezioni trattano i requisiti per l'utilizzo delle politiche firewall DNS di Firewall Manager e descrivono come funzionano le politiche. Per la procedura di creazione della policy, vedereCreazione di una AWS Firewall Manager policy per Amazon Route 53 Resolver DNS Firewall.

È necessario abilitare la condivisione delle risorse

Una policy DNS Firewall condivide i gruppi di regole del firewall DNS tra gli account dell'organizzazione. Affinché funzioni, è necessario che la condivisione delle risorse sia abilitata con. AWS Organizations Per informazioni su come abilitare la condivisione delle risorse, vedereCondivisione delle risorse per le politiche Network Firewall e DNS Firewall.

È necessario che i gruppi di regole del firewall DNS siano definiti

Quando specifichi una nuova policy DNS Firewall, definisci i gruppi di regole nello stesso modo in cui utilizzi direttamente Amazon Route 53 Resolver DNS Firewall. I gruppi di regole devono già esistere

nell'account amministratore di Firewall Manager per poterli includere nella policy. Per informazioni sulla creazione di gruppi di regole del firewall DNS, consulta Gruppi e regole del firewall DNS.

L'utente definisce le associazioni dei gruppi di regole con priorità più bassa e più alta

Le associazioni dei gruppi di regole del firewall DNS che gestisci tramite le politiche del firewall DNS di Firewall Manager contengono le associazioni con priorità più bassa e le associazioni con priorità più alta per i tuoi VPC. Nella configurazione delle policy, queste appaiono come primo e ultimo gruppo di regole.

DNS Firewall filtra il traffico DNS per il VPC nel seguente ordine:

1. Primi gruppi di regole, definiti dall'utente nella politica Firewall DNS Firewall di Firewall Manager. I valori validi sono compresi tra 1 e 99.
2. Gruppi di regole DNS Firewall associati dai singoli account manager tramite DNS Firewall.
3. Ultimi gruppi di regole, definiti dall'utente nella politica Firewall DNS Firewall di Firewall Manager. I valori validi sono compresi tra 9901 e 10000.

Eliminazione di un gruppo di regole

Per eliminare un gruppo di regole da una policy Firewall DNS Firewall Manager, è necessario effettuare le seguenti operazioni:

1. Rimuovi il gruppo di regole dalla politica del firewall DNS di Firewall Manager.
2. Annulla la condivisione del gruppo di regole in. AWS Resource Access Manager Per annullare la condivisione di un gruppo di regole di cui sei proprietario, devi rimuoverlo dalla condivisione di risorse. Puoi farlo usando la AWS RAM console o la AWS CLI. Per informazioni sull'annullamento della condivisione di una risorsa, consulta Aggiornare una condivisione di risorse AWS RAM nella Guida per l'AWS RAM utente.
3. Eliminare il gruppo di regole utilizzando la console DNS Firewall o la AWS CLI.

Come Firewall Manager nomina le associazioni di gruppi di regole che crea

Quando salvi la policy DNS Firewall, se hai abilitato il ripristino automatico, Firewall Manager crea un'associazione DNS Firewall tra i gruppi di regole forniti nella policy e i VPC che rientrano nell'ambito della policy. Firewall Manager assegna un nome a queste associazioni concatenando i seguenti valori:

- La stringa fissa,. `FMManaged_`
- L'ID della politica di Firewall Manager. Questo è l'ID della AWS risorsa per la policy Firewall Manager.

Di seguito viene illustrato un esempio di nome per un firewall gestito da Firewall Manager:

```
FMManaged_EXAMPLEDNSFirewallPolicyId
```

Dopo aver creato la policy, se i proprietari degli account nei VPC sovrascrivono le impostazioni delle policy del firewall o le associazioni dei gruppi di regole, Firewall Manager contrassegnerà la policy come non conforme e proverà a proporre un'azione correttiva. I proprietari degli account possono associare altri gruppi di regole DNS Firewall ai VPC che rientrano nell'ambito della politica DNS Firewall. Tutte le associazioni create dai singoli proprietari degli account devono avere impostazioni di priorità tra la prima e l'ultima associazione dei gruppi di regole.

Politiche NGFW di Palo Alto Networks Cloud

Il Palo Alto Networks Cloud Next Generation Firewall (NGFW) è un servizio firewall di terze parti che puoi utilizzare per le tue policy. AWS Firewall Manager Con Palo Alto Networks Cloud NGFW for Firewall Manager, puoi creare e distribuire centralmente risorse e set di regole NGFW di Palo Alto Networks Cloud su tutti i tuoi account. AWS

Per utilizzare Palo Alto Networks Cloud NGFW con Firewall Manager, devi prima abbonarti al servizio Palo Alto Networks Cloud NGFW Pay-As-You-Go nel Marketplace. AWS Dopo la sottoscrizione, esegui una serie di passaggi nel servizio Palo Alto Networks Cloud NGFW per configurare il tuo account e le impostazioni Cloud NGFW. Quindi, crei una policy Firewall Manager Cloud FMS per distribuire e gestire centralmente le risorse e le regole NGFW di Palo Alto Networks Cloud in tutti gli account delle tue Organizzazioni. AWS

Per la procedura di creazione della policy Firewall Manager, vedereCreazione di una AWS Firewall Manager policy per Palo Alto Networks Cloud NGFW. Per informazioni su come configurare e gestire Palo Alto Networks Cloud NGFW for Firewall Manager, vedere Palo Alto Networks Palo Alto Networks Cloud NGFW sulla documentazione. AWS

Politiche di Fortigate Cloud Native Firewall (CNF) as a Service

Fortigate Cloud Native Firewall (CNF) as a Service è un servizio firewall di terze parti che puoi utilizzare per le tue politiche. AWS Firewall Manager Fortigate CNF è un servizio firewall di nuova

generazione che semplifica la protezione delle reti cloud e la gestione delle politiche di sicurezza. Con Fortigate CNF for Firewall Manager, puoi creare e distribuire centralmente risorse e set di policy Fortigate CNF su tutti i tuoi account. AWS

Per utilizzare Fortigate CNF con Firewall Manager, devi prima abbonarti al Fortigate Cloud Native Firewall (CNF) as a Service nel Marketplace. AWS Dopo l'iscrizione, esegui una serie di passaggi nel servizio Fortigate CNF per configurare i set di policy globali e altre impostazioni. Quindi, crei una policy Firewall Manager per distribuire e gestire centralmente le risorse Fortigate CNF su tutti gli account delle tue Organizations. AWS

Per la procedura per la creazione di una policy Fortigate CNF Firewall Manager, vedere. Creazione di una AWS Firewall Manager policy per Fortigate Cloud Native Firewall (CNF) as a Service Per informazioni su come configurare e gestire Fortigate CNF per l'utilizzo con Firewall Manager, consulta la documentazione di Fortigate CNF.

Condivisione delle risorse per le politiche Network Firewall e DNS Firewall

Per gestire le politiche Firewall Manager Network Firewall e DNS Firewall, è necessario abilitare la condivisione delle risorse con AWS Organizations in AWS Resource Access Manager. Ciò consente a Firewall Manager di implementare protezioni su tutti gli account quando si creano questi tipi di policy.

Per abilitare la condivisione delle risorse, segui le istruzioni riportate nella sezione Abilita la condivisione con AWS Organizations nella Guida per l'AWS Resource Access Manager utente.

Problemi con la condivisione delle risorse

Potresti riscontrare problemi con la condivisione delle risorse, sia quando la utilizzi AWS RAM per abilitarla, sia quando lavori sulle politiche di Firewall Manager che la richiedono.

Alcuni esempi di questi problemi sono i seguenti:

- Quando segui le istruzioni per abilitare la condivisione, nella AWS RAM console, la scelta Abilita condivisione con AWS Organizations è disattivata e non è disponibile per la selezione.
- Quando si lavora in Firewall Manager su una politica che richiede la condivisione delle risorse, la politica viene contrassegnata come non conforme e vengono visualizzati messaggi che indicano che la condivisione delle risorse AWS RAM è o non è abilitata.

Se si riscontrano problemi con la condivisione delle risorse, utilizzare la procedura seguente per provare ad abilitarla.

Riprova ad abilitare la condivisione delle risorse

- Riprova ad abilitare la condivisione utilizzando una delle seguenti opzioni:
  - (Opzione) Tramite la AWS RAM console, segui le istruzioni in Abilita la condivisione con AWS Organizations nella Guida per l'AWS Resource Access Manager utente.
  - (Opzione) Utilizzando l' AWS RAM API, chiama`EnableSharingWithAwsOrganization`. Consulta la documentazione all'indirizzo EnableSharingWithAwsOrganization.

Utilizzo dei set di risorse in Firewall Manager

Un set di AWS Firewall Manager risorse è una raccolta di risorse, come i firewall, che è possibile raggruppare e gestire in una politica di Firewall Manager. I set di risorse consentono ai membri dell'organizzazione di avere un controllo granulare sulle risorse da gestire in una policy. Per utilizzare i set di risorse, crea un set di risorse nella console o utilizzando l'PutResourceSetAPI, quindi aggiungi il set di risorse alla politica di Firewall Manager.

È possibile creare e gestire set di risorse per i seguenti tipi di risorse e policy di sicurezza:

Tipo di risorsa	Tipo di policy di sicurezza Firewall Manager
AWS Network Firewall - firewall	Politica Network Firewall: utilizza i set di risorse per importare i firewall esistenti da Network Firewall. Per informazioni sull'utilizzo dei set di risorse in una politica di Network Firewall, vedere il passaggio Importazione di firewall esistenti della Creazione di una AWS Firewall Manager politica per AWS Network Firewall procedura.

Nelle sezioni seguenti vengono descritti i requisiti per la creazione e l'eliminazione di set di risorse.

Argomenti

Considerazioni sull'utilizzo di set di risorse in Firewall Manager

Quando si lavora con i set di risorse, tenete presente le seguenti considerazioni

Riferimenti a risorse inesistenti

Quando aggiungi una risorsa a un set di risorse, crei un riferimento alla risorsa utilizzando un Amazon Resource Name (ARN). Firewall Manager verifica che Amazon Resource Name (ARN) sia il formato corretto, ma Firewall Manager non verifica l'esistenza della risorsa di riferimento. Se la risorsa non

esiste ancora supera la convalida ARN, Firewall Manager include il riferimento alla risorsa nel set di risorse. Se successivamente viene creata una nuova risorsa con lo stesso ARN, Firewall Manager applica i gruppi di regole dalla politica associata al set di risorse alla nuova risorsa.

Risorse eliminate

Quando una risorsa in un set di risorse viene eliminata, il riferimento alla risorsa rimane nel set di risorse finché non viene rimosso dall'amministratore di Firewall Manager.

Risorse di proprietà dell'account membro che lascia l' AWS Organizations organizzazione

Se un account membro lascia l'organizzazione, qualsiasi riferimento alle risorse di proprietà di quell'account membro rimarrà nel set di risorse ma non sarà più gestito da alcuna politica a cui è associato il set di risorse.

Associazione a più politiche

Un set di risorse può essere associato a più policy, ma non tutti i tipi di policy supportano più policy per la gestione della stessa risorsa. Per informazioni sugli scenari non supportati, consulta la documentazione relativa al tipo di policy specifico.

Creazione di set di risorse

Per creare un set di risorse (console)

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegli Set di risorse.
3. Scegli Crea set di risorse.
4. Per Nome del set di risorse, inserisci un nome descrittivo.
5. (Facoltativo) inserite una descrizione per il set di risorse.
6. Seleziona Successivo.

7. Per Scegli risorse, seleziona un ID AWS account, quindi seleziona Scegli risorse per aggiungere risorse possedute e gestite da questo account al set di risorse. Dopo aver selezionato le risorse, seleziona Aggiungi per aggiungere le risorse al set di risorse.
8. Seleziona Successivo.
9. Per i tag del set di risorse, aggiungi i tag di identificazione che desideri per il set di risorse. Per ulteriori informazioni, consultare l'articolo relativo all'utilizzo di Tag Editor .
10. Seleziona Successivo.
11. Rivedi il nuovo set di risorse. Per apportare eventuali modifiche, scegliere Edit (Modifica) nell'area che si desidera modificare. In questo modo si torna al passaggio corrispondente della creazione guidata. Quando sei soddisfatto del set di risorse, scegli Crea set di risorse.

Eliminazione di un set di risorse

Prima di poter eliminare un set di risorse, è necessario separare il set di risorse da tutte le politiche che utilizzano il set di risorse. È possibile dissociare i gruppi di risorse nella pagina di dettaglio della policy utilizzando la console o l'PutPolicyAPI.

Per eliminare un set di risorse (console)

1. Nel riquadro di navigazione, scegli Set di risorse.
2. Scegliete l'opzione accanto al set di risorse che desiderate eliminare.
3. Scegli Delete (Elimina).

Visualizzazione delle informazioni sulla conformità per una AWS Firewall Manager politica

Questa sezione fornisce indicazioni per la visualizzazione dello stato di conformità degli account e delle risorse che rientrano nell'ambito di una AWS Firewall Manager politica. Per informazioni sui controlli in atto AWS per mantenere la sicurezza e la conformità del cloud, consultaConvalida della conformità per Firewall Manager.

> **Note**
>
> Affinché Firewall Manager possa monitorare la conformità delle policy, AWS Config deve registrare continuamente le modifiche alla configurazione per le risorse protette. Nella AWS

Config configurazione, la frequenza di registrazione deve essere impostata su Continuo, che è l'impostazione predefinita.

> **Note**
>
> Per mantenere uno stato di conformità adeguato nelle risorse protette, evita di modificare ripetutamente lo stato delle protezioni di Firewall Manager, automaticamente o manualmente. Firewall Manager utilizza le informazioni di AWS Config per rilevare le modifiche alle configurazioni delle risorse. Se le modifiche vengono applicate abbastanza rapidamente, si AWS Config può perdere di vista alcune di esse, con conseguente perdita di informazioni sulla conformità o sullo stato di riparazione in Firewall Manager.
> Se noti che uno stato di conformità o riparazione di una risorsa che stai proteggendo con Firewall Manager non è corretto, assicurati innanzitutto di non eseguire alcun processo che alteri o ripristini le protezioni di Firewall Manager, quindi aggiorna il AWS Config tracciamento della risorsa rivalutando le regole di configurazione associate in. AWS Config

Per tutte le AWS Firewall Manager politiche, puoi visualizzare lo stato di conformità degli account e delle risorse che rientrano nell'ambito della politica. Un account o una risorsa è conforme a una politica di Firewall Manager se le impostazioni della politica si riflettono nelle impostazioni dell'account o della risorsa. Ogni tipo di policy ha i propri requisiti di conformità, che è possibile regolare al momento della definizione della policy. Per alcune politiche, puoi anche visualizzare informazioni dettagliate sulle violazioni relative alle risorse pertinenti, per aiutarti a comprendere e gestire meglio i rischi per la sicurezza.

Per visualizzare le informazioni sulla conformità di una politica

1. Accedi AWS Management Console utilizzando il tuo account amministratore di Firewall Manager, quindi apri la console Firewall Manager all'indirizzohttps://console.aws.amazon.com/wafv2/fmsv2. Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

   > **Note**
   >
   > Per ulteriori informazioni sulla configurazione di un account amministratore di Firewall Manager, consultare AWS Firewall Manager prerequisiti.

2. Nel riquadro di navigazione, scegliere Security policies (Policy di sicurezza).
3. Scegliere una policy. Nella scheda Account e risorse della pagina dei criteri, Firewall Manager elenca gli account dell'organizzazione, raggruppati in base a quelli che rientrano nell'ambito della politica e quelli che non rientrano nell'ambito della politica.

   Il riquadro Account rientranti nell'ambito della policy elenca lo stato di conformità di ogni account. Lo stato Conforme indica che la politica è stata applicata correttamente a tutte le risorse relative all'account. Lo stato Non conforme indica che la politica non è stata applicata a una o più risorse relative all'account.
4. Scegli un account non conforme. Nella pagina dell'account, Firewall Manager elenca l'ID e il tipo di ogni risorsa non conforme e il motivo per cui la risorsa viola la politica.

   > **Note**
   >
   > Per i tipi di risorse `AWS::EC2::NetworkInterface` (ENI) e`AWS::EC2::Instance`, Firewall Manager potrebbe mostrare un numero limitato di risorse non conformi. Per elencare altre risorse non conformi, correggi quelle inizialmente visualizzate per l'account.
5. Se il tipo di policy di Firewall Manager è un criterio di gruppo di sicurezza per il controllo dei contenuti, è possibile accedere a informazioni dettagliate sulle violazioni relative a una risorsa.

   Per visualizzare i dettagli della violazione, scegli la risorsa.

   > **Note**
   >
   > Le risorse che Firewall Manager ha ritenuto non conformi prima dell'aggiunta della pagina dettagliata sulla violazione delle risorse potrebbero non avere dettagli sulla violazione.

   Nella pagina delle risorse, Firewall Manager elenca dettagli specifici sulla violazione, in base al tipo di risorsa.

   - **`AWS::EC2::NetworkInterface`**(ENI): Firewall Manager visualizza informazioni sul gruppo di sicurezza a cui la risorsa non è conforme. Scegli il gruppo di sicurezza per visualizzarne maggiori dettagli.

- **`AWS::EC2::Instance`**— Firewall Manager visualizza l'ENI collegato all'istanza EC2 che non è conforme. Visualizza anche informazioni sul gruppo di sicurezza a cui le risorse non sono conformi. Scegli il gruppo di sicurezza per visualizzarne maggiori dettagli.
- **`AWS::EC2::SecurityGroup`**— Firewall Manager visualizza i seguenti dettagli sulla violazione:
  - Regola del gruppo di sicurezza non conforme: la regola violata, inclusi il protocollo, l'intervallo di porte, l'intervallo IP CIDR e la descrizione.
  - Regola di riferimento: la regola del gruppo di sicurezza di controllo violata dalla regola del gruppo di sicurezza non conforme, con i relativi dettagli.
  - Motivi della violazione: spiegazione dell'accertamento di non conformità.
  - Azione correttiva: azione suggerita da intraprendere. Se Firewall Manager non è in grado di determinare un'azione di riparazione sicura, questo campo è vuoto.
- **`AWS::EC2::Subnet`**— Viene utilizzato per le politiche del Network Firewall. Firewall Manager visualizza l'ID di sottorete, l'ID VPC e la zona di disponibilità. Se applicabile, Firewall Manager include informazioni aggiuntive sulla violazione, ad esempio il motivo per cui si è verificata la violazione o l'ID della tabella di routing a cui deve essere associata una sottorete. Il componente di descrizione della violazione contiene una descrizione dello stato previsto della risorsa, dello stato attuale non conforme e, se disponibile, una descrizione della causa della discrepanza.

  Ad esempio, lo stato previsto di una sottorete potrebbe essere «La sottorete dovrebbe contenere una AWS Network Firewall sottorete nella sua zona di disponibilità», lo stato corrente potrebbe essere «alla sottorete con id subnet-1234 manca una sottorete Network Firewall nella zona di disponibilità us-east-1e» e la descrizione potrebbe essere «Firewall Manager non è riuscito a creare una sottorete in questa zona di disponibilità perché non ci sono blocchi CIDR disponibili».
  - Violazioni della gestione delle rotte: per le politiche del firewall di rete che utilizzano la modalità Monitor, Firewall Manager visualizza le informazioni di base sulla sottorete, nonché le route previste ed effettive nella sottorete, nel gateway Internet e nella tabella di routing della sottorete Network Firewall. Firewall Manager avvisa l'utente che c'è una violazione se le route effettive non corrispondono alle route previste nella tabella delle rotte.
  - Azioni di riparazione per le violazioni della gestione delle rotte: per le politiche del Network Firewall che utilizzano la modalità Monitor, Firewall Manager suggerisce possibili azioni di riparazione sulle configurazioni di routing che presentano violazioni.

Example — Violazioni nella gestione delle rotte e suggerimenti per la correzione

Si prevede che una sottorete invii il traffico attraverso gli endpoint del firewall, ma la sottorete attuale invia il traffico direttamente al gateway Internet. Si tratta di una violazione della gestione del percorso. La soluzione suggerita in questo caso potrebbe essere un elenco di azioni ordinate. La prima è una raccomandazione di aggiungere le route richieste alla tabella di routing della sottorete Network Firewall per indirizzare il traffico in uscita verso il gateway Internet e per indirizzare il traffico in entrata verso le destinazioni all'interno del VPC. `local` La seconda raccomandazione consiste nel sostituire la route del gateway Internet o la route Network Firewall non valida nella tabella di routing della sottorete per indirizzare il traffico in uscita verso gli endpoint del firewall. La terza raccomandazione consiste nell'aggiungere i percorsi richiesti alla tabella di routing del gateway Internet per indirizzare il traffico in entrata verso gli endpoint del firewall.

- **`AWS::EC2::InternetGateway`**— Viene utilizzato per le politiche Network Firewall che hanno la modalità Monitor abilitata.
  - Violazioni della gestione delle rotte: il gateway Internet non è conforme se il gateway Internet non è associato a una tabella di routing o se nella tabella di routing del gateway Internet è presente una route non valida.
  - Azioni di riparazione per le violazioni della gestione delle rotte: Firewall Manager suggerisce possibili azioni di riparazione per porre rimedio alle violazioni della gestione delle rotte.

  Example 1 — Violazione della gestione del percorso e suggerimenti per la correzione

  Un gateway Internet non è associato a una tabella di routing. Le azioni correttive suggerite potrebbero essere un elenco di azioni ordinate. La prima azione consiste nel creare una tabella di rotte. La seconda azione consiste nell'associare la tabella delle rotte al gateway Internet. La terza azione consiste nell'aggiungere la route richiesta alla tabella di routing del gateway Internet.

  Example 2 — Violazione della gestione del percorso e suggerimenti per la riparazione

  Il gateway Internet è associato a una tabella di routing valida, ma la route è configurata in modo errato. La correzione suggerita potrebbe essere un elenco di azioni ordinate. Il primo suggerimento è quello di rimuovere la rotta non valida. Il secondo consiste nell'aggiungere la route richiesta alla tabella delle rotte del gateway Internet.
- **`AWS::NetworkFirewall::FirewallPolicy`**— Viene utilizzato per le politiche del Network Firewall. Firewall Manager visualizza informazioni su una politica firewall di Network Firewall

che è stata modificata in modo da renderla non conforme. Le informazioni forniscono la politica firewall prevista e la politica trovata nell'account cliente, in modo da poter confrontare i nomi e le impostazioni di priorità dei gruppi di regole stateless e stateful, i nomi delle azioni personalizzate e le impostazioni predefinite delle azioni senza stato. Il componente di descrizione della violazione contiene una descrizione dello stato previsto della risorsa, dello stato attuale non conforme e, se disponibile, una descrizione della causa della discrepanza.

- **`AWS::EC2::VPC`**— Viene utilizzato per le politiche del firewall DNS. Firewall Manager visualizza informazioni su un VPC che rientra nell'ambito di una policy Firewall DNS Firewall di Firewall Manager e che non è conforme alla policy. Le informazioni fornite includono i gruppi di regole previsti che dovrebbero essere associati al VPC e i gruppi di regole effettivi. Il componente di descrizione della violazione contiene una descrizione dello stato previsto della risorsa, dello stato attuale non conforme e, se disponibile, una descrizione della causa della discrepanza.

AWS Firewall Manager scoperte

AWS Firewall Manager crea i risultati relativi alle risorse che non sono conformi e agli attacchi rilevati e li invia a AWS Security Hub. Per informazioni sui risultati di Security Hub, vedere Findings in AWS Security Hub.

Quando si utilizzano Security Hub e Firewall Manager, Firewall Manager invia automaticamente i risultati a Security Hub. Per informazioni su come iniziare a usare Security Hub, consulta Configurazione AWS Security Hub nella Guida AWS Security Hub per l'utente.

Come posso visualizzare i risultati del mio Firewall Manager?

Per visualizzare i risultati di Firewall Manager in Security Hub, segui le indicazioni in Working with Findings in Security Hub e crea un filtro utilizzando le seguenti impostazioni:

- Attributo impostato su Product Name (Nome prodotto).
- Operatore impostato su EQUALS.
- Valore impostato su `Firewall Manager`. Questa impostazione fa distinzione tra maiuscole e minuscole.

Posso disabilitare questo?

È possibile disabilitare l'integrazione dei AWS Firewall Manager risultati con Security Hub tramite la console Security Hub. Scegli Integrazioni nella barra di navigazione, quindi nel riquadro Firewall Manager, scegli Disabilita integrazione. Per ulteriori informazioni, consulta la AWS Security Hub Guida per l'utente.

AWS Firewall Manager Individuazione dei tipi

- AWS WAF risultati politici
- AWS Shield Advanced risultati politici
- Risultati delle policy comuni dei gruppi di sicurezza
- Risultati delle policy di controllo del contenuto dei gruppi di sicurezza.
- Risultati delle policy di controllo dell'utilizzo dei gruppi di sicurezza
- Risultati della politica del firewall DNS di Amazon Route 53 Resolver

AWS WAF risultati politici

È possibile utilizzare AWS WAF le politiche di Firewall Manager per applicare gruppi di AWS WAF regole alle risorse in AWS Organizations. Per ulteriori informazioni, consulta Lavorare con AWS Firewall Manager le politiche.

Nella risorsa manca l'ACL web gestito da Firewall Manager.

Una AWS risorsa non dispone dell'associazione ACL Web AWS Firewall Manager gestita in conformità con la politica di Firewall Manager. È possibile abilitare la correzione di Firewall Manager sulla policy per correggere questo problema.

- Severità: 80
- Impostazioni di stato: SUPERATO/NON RIUSCITO
- Aggiornamenti: se Firewall Manager esegue l'azione di riparazione, aggiornerà il risultato e la gravità diminuirà da `HIGH` a`INFORMATIONAL`. Se si esegue la riparazione, Firewall Manager non aggiornerà il risultato.

L'ACL Web gestito da Firewall Manager presenta gruppi di regole configurati in modo errato.

I gruppi di regole in un ACL Web gestito da Firewall Manager non sono configurati correttamente, in base alla politica di Firewall Manager. Ciò significa che all'ACL Web mancano i gruppi di regole

richiesti dalla policy. È possibile abilitare la correzione di Firewall Manager sulla policy per correggere questo problema.

- Severità: 80
- Impostazioni di stato: SUPERATO/NON RIUSCITO
- Aggiornamenti: se Firewall Manager esegue l'azione di riparazione, aggiornerà il risultato e la gravità diminuirà da `HIGH` a`INFORMATIONAL`. Se si esegue la riparazione, Firewall Manager non aggiornerà il risultato.

AWS Shield Advanced risultati politici

Per informazioni sulle AWS Shield Advanced politiche, vederePolitiche dei gruppi di sicurezza.

La risorsa non dispone della protezione Shield Advanced.

Una AWS risorsa che dovrebbe avere la protezione Shield Advanced, secondo la politica di Firewall Manager, non la possiede. È possibile abilitare la correzione di Firewall Manager sulla policy, che abiliterà la protezione della risorsa.

- Severità: 60
- Impostazioni di stato: SUPERATO/NON RIUSCITO
- Aggiornamenti: se Firewall Manager esegue l'azione di riparazione, aggiornerà il risultato e la gravità diminuirà da `HIGH` a`INFORMATIONAL`. Se si esegue la riparazione, Firewall Manager non aggiornerà il risultato.

Shield Advanced ha rilevato un attacco contro una risorsa monitorata.

Shield Advanced ha rilevato un attacco a una AWS risorsa protetta. È possibile abilitare la correzione di Firewall Manager sulla policy.

- Severità: 70
- Impostazioni di stato: nessuna
- Aggiornamenti: Firewall Manager non aggiorna questo risultato.

Risultati delle policy comuni dei gruppi di sicurezza

Per informazioni sulle policy comuni dei gruppi di sicurezza, consultare Politiche dei gruppi di sicurezza.

La risorsa ha configurato in modo errato il gruppo di sicurezza.

Firewall Manager ha identificato una risorsa a cui mancano le associazioni dei gruppi di sicurezza gestiti di Firewall Manager che dovrebbe avere, in base alla politica di Firewall Manager. È possibile abilitare la correzione di Firewall Manager sulla policy, che crea le associazioni in base alle impostazioni delle policy.

- Severità: 70
- Impostazioni di stato: SUPERATO/NON RIUSCITO
- Aggiornamenti: Firewall Manager aggiorna questo risultato.

Il gruppo di sicurezza di replica di Firewall Manager non è sincronizzato con il gruppo di sicurezza primario.

Un gruppo di sicurezza di replica di Firewall Manager non è sincronizzato con il gruppo di sicurezza principale, in base alla politica comune del gruppo di sicurezza. È possibile abilitare la correzione di Firewall Manager sulla policy, che sincronizza i gruppi di sicurezza delle repliche con quelli primari.

- Severità: 80
- Impostazioni di stato: SUPERATO/NON RIUSCITO
- Aggiornamenti: Firewall Manager aggiorna questo risultato.

Risultati delle policy di controllo del contenuto dei gruppi di sicurezza.

Per informazioni sulle policy di controllo del contenuto dei gruppi di sicurezza, consultare Politiche dei gruppi di sicurezza.

Il gruppo di sicurezza non è conforme al gruppo di sicurezza per il controllo del contenuto.

Un criterio di controllo dei contenuti del gruppo di sicurezza Firewall Manager ha identificato un gruppo di sicurezza non conforme. Si tratta di un gruppo di sicurezza creato dal cliente che rientra nell'ambito della policy di controllo del contenuto e che non è conforme alle impostazioni definite dalla

policy e dal relativo gruppo di sicurezza di controllo. È possibile abilitare la correzione di Firewall Manager sulla policy, che modifica il gruppo di sicurezza non conforme per renderlo conforme.

- Severità: 70
- Impostazioni di stato: SUPERATO/FALLITO
- Aggiornamenti: Firewall Manager aggiorna questo risultato.

Risultati delle policy di controllo dell'utilizzo dei gruppi di sicurezza

Per informazioni sulle policy di controllo dell'utilizzo dei gruppi di sicurezza, consultare Politiche dei gruppi di sicurezza.

Firewall Manager ha rilevato un gruppo di sicurezza ridondante.

Il controllo dell'utilizzo del gruppo di sicurezza Firewall Manager ha identificato un gruppo di sicurezza ridondante. Si tratta di un gruppo di sicurezza con regole identiche a quelle di un altro gruppo di sicurezza all'interno della stessa istanza di Amazon Virtual Private Cloud. È possibile abilitare la correzione automatica di Firewall Manager sulla politica di controllo dell'utilizzo, che sostituisce i gruppi di sicurezza ridondanti e con un singolo gruppo di sicurezza.

- Severità: 30
- Impostazioni di stato: nessuna
- Aggiornamenti: Firewall Manager non aggiorna questo risultato.

Firewall Manager ha rilevato un gruppo di sicurezza inutilizzato.

Il controllo dell'utilizzo del gruppo di sicurezza Firewall Manager ha identificato un gruppo di sicurezza inutilizzato. Si tratta di un gruppo di sicurezza a cui non fa riferimento alcuna politica di gruppo di sicurezza comune di Firewall Manager. È possibile abilitare la correzione automatica di Firewall Manager sulla politica di controllo dell'utilizzo, che rimuove i gruppi di sicurezza non utilizzati.

- Severità: 30
- Impostazioni di stato: nessuna
- Aggiornamenti: Firewall Manager non aggiorna questo risultato.

Risultati della politica del firewall DNS di Amazon Route 53 Resolver

Per informazioni sulle politiche del firewall DNS, consulta. Politiche del firewall DNS di Amazon Route 53 Resolver

Nella risorsa manca la protezione DNS Firewall

A un VPC manca un'associazione di gruppi di regole DNS Firewall definita nella policy Firewall DNS Firewall di Firewall Manager. Il risultato elenca il gruppo di regole specificato dalla policy.

- Severità: 80

Sicurezza in AWS Firewall Manager

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. L'efficacia della nostra sicurezza è regolarmente testata e verificata da revisori di terze parti come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità che si applicano a Firewall Manager, vedere AWS Servizi compresi nell'ambito del programma di conformità.
- Sicurezza nel cloud: la responsabilità dell'utente è determinata dal AWS servizio utilizzato. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e leggi e normative applicabili.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza Firewall Manager. I seguenti argomenti mostrano come configurare Firewall Manager per soddisfare gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse di Firewall Manager.

Argomenti

- Protezione dei dati in Firewall Manager

- Identity and Access Management per AWS Firewall Manager
- Registrazione e monitoraggio in Firewall Manager
- Convalida della conformità per Firewall Manager
- Resilienza in Firewall Manager
- Sicurezza dell'infrastruttura nell' AWS Firewall Manager

Protezione dei dati in Firewall Manager

Il modello di responsabilità AWS di si applica alla protezione dei dati in AWS Firewall Manager. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Firewall Manager o altro Servizi AWS utilizzando la console, l'API o AWS

gli SDK. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Le entità Firewall Manager, come le policy, sono crittografate quando sono inattive, tranne in alcune regioni in cui la crittografia non è disponibile, tra cui Cina (Pechino) e Cina (Ningxia). Per ogni regione vengono utilizzate chiavi di crittografia univoche.

Identity and Access Management per AWS Firewall Manager

AWS Identity and Access Management (IAM) aiuta un Servizio AWS amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (dispone delle autorizzazioni) a utilizzare le risorse di Firewall Manager. IAM è un Servizio AWS software che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Firewall Manager.

Utente del servizio: se si utilizza il servizio Firewall Manager per svolgere il proprio lavoro, l'amministratore fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Firewall Manager per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni

aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non è possibile accedere a una funzionalità di Firewall Manager, vedereRisoluzione dei problemi di AWS Shield identità e accesso.

Amministratore del servizio: se sei responsabile delle risorse di Firewall Manager presso la tua azienda, probabilmente hai pieno accesso a Firewall Manager. È compito dell'utente determinare a quali funzionalità e risorse di Firewall Manager devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Firewall Manager, consultaCome AWS Shield funziona con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso a Firewall Manager. Per visualizzare esempi di policy basate sull'identità di Firewall Manager che puoi utilizzare in IAM, consulta. Esempi di policy basate su identità per AWS Shield

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le

chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.

- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori

informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'azione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruoli IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS.

Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.

- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per sapere come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come AWS Firewall Manager funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a Firewall Manager, scopri quali funzionalità IAM sono disponibili per l'uso con Firewall Manager.

Funzionalità IAM che puoi utilizzare con AWS Firewall Manager

Funzionalità IAM	Supporto Firewall Manager
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì

Funzionalità IAM	Supporto Firewall Manager
Chiavi di condizione della policy (specifica del servizio)	No
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	Parziale
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come Firewall Manager e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per Firewall Manager

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Per visualizzare esempi di policy basate sull'identità di Firewall Manager, vedere. Esempi di policy basate sull'identità per AWS Firewall Manager

Esempi di policy basate sull'identità per Firewall Manager

Per visualizzare esempi di policy basate sull'identità di Firewall Manager, vedere. Esempi di policy basate sull'identità per AWS Firewall Manager

Politiche basate sulle risorse all'interno di Firewall Manager

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Azioni politiche per Firewall Manager

Supporta le azioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni di Firewall Manager, vedere Azioni definite da AWS Firewall Manager nel Service Authorization Reference.

Le azioni relative alle policy in Firewall Manager utilizzano il seguente prefisso prima dell'azione:

```
fms
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "fms:action1",
      "fms:action2"
         ]
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Describe`, includi la seguente azione:

```
"Action": "fms:Describe*"
```

Per visualizzare esempi di policy basate sull'identità di Firewall Manager, vedere. Esempi di policy basate sull'identità per AWS Firewall Manager

Risorse relative alle policy per Firewall Manager

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di risorse di Firewall Manager e dei relativi ARN, vedere Risorse definite da AWS Firewall Manager nel Service Authorization Reference. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta la sezione Operazioni definite da AWS Firewall Manager.

Per visualizzare esempi di policy basate sull'identità di Firewall Manager, vedere. Esempi di policy basate sull'identità per AWS Firewall Manager

Chiavi delle condizioni delle policy per Firewall Manager

Supporta le chiavi di condizione delle policy specifiche del servizio	No

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione

logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco delle chiavi di condizione di Firewall Manager, vedere Chiavi di condizione AWS Firewall Manager nel Service Authorization Reference. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, vedere Azioni definite da AWS Firewall Manager.

Per visualizzare esempi di policy basate sull'identità di Firewall Manager, vedere. Esempi di policy basate sull'identità per AWS Firewall Manager

ACL in Firewall Manager

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con Firewall Manager

Supporta ABAC (tag nelle policy)	Sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Firewall Manager

Supporta le credenziali temporanee	Sì

Alcune Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Sessioni di accesso diretto per Firewall Manager

Supporta sessioni di accesso diretto (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

Ruoli di servizio per Firewall Manager

Supporta i ruoli di servizio	Parziale

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di Firewall Manager. Modifica i ruoli di servizio solo quando Firewall Manager fornisce indicazioni in tal senso.

Scelta di un ruolo IAM in Firewall Manager

Per utilizzare l'azione *`PutNotificationChannel`*API in Firewall Manager, devi scegliere un ruolo per consentire a Firewall Manager di accedere ad Amazon SNS in modo che il servizio possa pubblicare messaggi Amazon SNS per tuo conto. Per ulteriori informazioni, consulta l'AWS Firewall Manager API PutNotificationChannelReference.

Di seguito viene illustrato un esempio di impostazione delle autorizzazioni per gli argomenti SNS. Per utilizzare questa politica con il tuo ruolo personalizzato, sostituisci `AWSServiceRoleForFMS` Amazon Resource Name (ARN) con l'`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"
}
```

Per ulteriori informazioni sulle azioni e le risorse di Firewall Manager, vedere l'argomento della AWS Identity and Access Management guida Azioni definite da AWS Firewall Manager

Ruoli collegati ai servizi per Firewall Manager

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati in Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per AWS Firewall Manager

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare le risorse di Firewall Manager. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da Firewall Manager, incluso il formato degli ARN per ciascun tipo di risorsa, vedere Azioni, risorse e chiavi di condizione AWS Firewall Manager nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console Firewall Manager
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Concedi l'accesso in lettura ai tuoi gruppi di sicurezza Firewall Manager
- Concessione dell'accesso completo alle risorse AWS Firewall Manager

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse di Firewall Manager nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso ad azioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Firewall Manager

Per accedere alla AWS Firewall Manager console, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentire di elencare e visualizzare i dettagli sulle risorse di Firewall Manager presenti nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario concedere autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la console Firewall Manager, collega anche Firewall Manager *ConsoleAccess* o la policy *ReadOnly* AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI 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": "*"
        }
    ]
}
```

Concedi l'accesso in lettura ai tuoi gruppi di sicurezza Firewall Manager

Firewall Manager consente l'accesso alle risorse tra account, ma non consente di creare protezioni delle risorse tra account. È possibile creare protezioni per le risorse solo dall'interno dell'account proprietario di tali risorse.

Di seguito è riportato un esempio di politica che concede autorizzazioni per e `ec2:DescribeSecurityGroups` azioni su `fms:Get` tutte `fms:List` le risorse.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Action": [
                "fms:Get*",
                "fms:List*",
                "ec2:DescribeSecurityGroups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Concessione dell'accesso completo alle risorse AWS Firewall Manager

Segui questa guida se hai difficoltà a creare o gestire le policy di Firewall Manager con la policy gestita,`AWSFMAdminFullAccess`. Per informazioni sull'utilizzo delle politiche gestite per AWS Firewall Manager, vedere.

Questa politica non include le autorizzazioni per la configurazione delle notifiche di Amazon Simple Notification Service in AWS Firewall Manager. Per informazioni su come configurare l'accesso per Amazon Simple Notification Service, consulta Configurazione dell'accesso per Amazon Simple Notification Service.

Utilizza la seguente politica per concedere l'accesso amministrativo completo al tuo account:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "fms:*",
            "waf:*",
            "waf-regional:*",
            "elasticloadbalancing:SetWebACL",
            "firehose:ListDeliveryStreams",
            "organizations:DescribeAccount",
            "organizations:DescribeOrganization",
            "organizations:ListRoots",
            "organizations:ListChildren",
            "organizations:ListAccounts",
            "organizations:ListAccountsForParent",
            "organizations:ListOrganizationalUnitsForParent",
```

```
            "shield:GetSubscriptionState",
            "route53resolver:ListFirewallRuleGroups",
            "route53resolver:GetFirewallRuleGroup",
            "wafv2:ListRuleGroups",
            "wafv2:ListAvailableManagedRuleGroups",
            "wafv2:CheckCapacity",
            "wafv2:PutLoggingConfiguration",
            "wafv2:ListAvailableManagedRuleGroupVersions",
            "network-firewall:DescribeRuleGroup",
            "network-firewall:DescribeRuleGroupMetadata",
            "network-firewall:ListRuleGroups",
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeRegions"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutBucketPolicy",
            "s3:GetBucketPolicy"
         ],
         "Resource":[
            "arn:aws:s3:::aws-waf-logs-*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":"iam:CreateServiceLinkedRole",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "iam:AWSServiceName":[
                  "fms.amazonaws.com"
               ]
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "organizations:EnableAWSServiceAccess",
            "organizations:ListDelegatedAdministrators",
            "organizations:RegisterDelegatedAdministrator",
```

```
            "organizations:DeregisterDelegatedAdministrator"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "organizations:ServicePrincipal":[
                  "fms.amazonaws.com"
               ]
            }
         }
      }
   ]
}
```

Dettagli delle autorizzazioni

Questa politica include le seguenti autorizzazioni. :

- `fms:*`:

  Consente di lavorare con AWS Firewall Manager le risorse.

- `waf:*`, `waf-regional:*`:

  Consente di lavorare con AWS WAF le politiche.

- `waf:*`, `waf-regional:*`:

  Consente di lavorare con AWS WAF le politiche.

- `elasticloadbalancing:SetWebACL`:

  Consente di associare elenchi di controllo degli accessi Web (ACL) a Elastic Load Balancers.

- `firehose:ListDeliveryStreams`:

  Consente di visualizzare i log. AWS WAF

- `organizations:DescribeAccount`, `organizations:DescribeOrganization`, `organizations:ListRoots`, `organizations:ListChildren`, `organizations:ListAccounts`, `organizations:ListAccountsForParent`, `organizations:ListOrganizationalUnitsForParent`:

  Ti consente di lavorare con AWS Organizations.

- `shield:GetSubscriptionState`:

Consente di visualizzare lo stato dell'abbonamento a una AWS Shield politica.

- `route53resolver:ListFirewallRuleGroups`, `route53resolver:GetFirewallRuleGroup`:

  Consente di utilizzare i gruppi di regole Route 53 Private DNS for VPC in base a una policy Route 53 Private DNS for VPC.

- `wafv2:ListRuleGroups`, `wafv2:ListAvailableManagedRuleGroups`, `wafv2:CheckCapacity`, `wafv2:PutLoggingConfiguration`, `wafv2:ListAvailableManagedRuleGroupVersions`:

  Consente di lavorare con le politiche. AWS WAFV2

- `network-firewall:DescribeRuleGroup`, `network-firewall:DescribeRuleGroupMetadata`, `network-firewall:ListRuleGroups`:

  Consente di lavorare con AWS Network Firewall le politiche.

- `ec2:DescribeAvailabilityZones`:

  Consente di visualizzare le zone di disponibilità di una AWS Network Firewall politica.

- `ec2:DescribeRegions`:

  Consente di visualizzare la regione di una politica nella AWS Firewall Manager console.

AWS politiche gestite per AWS Firewall Manager

Una policy AWS gestita è una policy autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità

principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AWS politica gestita: AWSFMAdminFullAccess

Utilizza la policy `AWSFMAdminFullAccess` AWS gestita per consentire agli amministratori di accedere alle AWS Firewall Manager risorse, inclusi tutti i tipi di policy di Firewall Manager. Questa politica non include le autorizzazioni per la configurazione delle notifiche di Amazon Simple Notification Service in AWS Firewall Manager. Per informazioni su come configurare l'accesso per Amazon Simple Notification Service, consulta Configurazione dell'accesso per Amazon Simple Notification Service.

Dettagli sulle autorizzazioni

Questa politica è raggruppata in istruzioni basate sul set di autorizzazioni.

- AWS Firewall Manager risorse politiche: consente autorizzazioni amministrative complete per le risorse in AWS Firewall Manager, inclusi tutti i tipi di policy di Firewall Manager.
- Scrivi AWS WAF log su Amazon Simple Storage Service: consente a Firewall Manager di scrivere e leggere AWS WAF i log in Amazon S3.
- Crea ruolo collegato al servizio: consente all'amministratore di creare un ruolo collegato al servizio, che consente a Firewall Manager di accedere alle risorse di altri servizi per tuo conto. Questa autorizzazione consente di creare il ruolo collegato al servizio solo per l'utilizzo da parte di Firewall Manager. Per informazioni su come Firewall Manager utilizza i ruoli collegati ai servizi, vedereUtilizzo di ruoli collegati ai servizi per Firewall Manager.
- AWS Organizations— Consente agli amministratori di utilizzare Firewall Manager per un'organizzazione in AWS Organizations. Dopo aver abilitato l'accesso affidabile per Firewall Manager in AWS Organizations, i membri dell'account amministratore possono visualizzare i risultati in tutta l'organizzazione. Per informazioni sull'utilizzo AWS Organizations con AWS Firewall Manager, vedere Utilizzo AWS Organizations con altri AWS servizi nella Guida per l'AWS Organizations utente.

```
{
   "Version":"2012-10-17",
   "Statement":[
```

```
      {
         "Effect":"Allow",
         "Action":[
            "fms:*",
            "waf:*",
            "waf-regional:*",
            "elasticloadbalancing:SetWebACL",
            "firehose:ListDeliveryStreams",
            "organizations:DescribeAccount",
            "organizations:DescribeOrganization",
            "organizations:ListRoots",
            "organizations:ListChildren",
            "organizations:ListAccounts",
            "organizations:ListAccountsForParent",
            "organizations:ListOrganizationalUnitsForParent",
            "shield:GetSubscriptionState",
            "route53resolver:ListFirewallRuleGroups",
            "route53resolver:GetFirewallRuleGroup",
            "wafv2:ListRuleGroups",
            "wafv2:ListAvailableManagedRuleGroups",
            "wafv2:CheckCapacity",
            "wafv2:PutLoggingConfiguration",
            "wafv2:ListAvailableManagedRuleGroupVersions",
            "network-firewall:DescribeRuleGroup",
            "network-firewall:DescribeRuleGroupMetadata",
            "network-firewall:ListRuleGroups",
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeRegions"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutBucketPolicy",
            "s3:GetBucketPolicy"
         ],
         "Resource":[
            "arn:aws:s3:::aws-waf-logs-*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":"iam:CreateServiceLinkedRole",
```

```
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "iam:AWSServiceName":[
                  "fms.amazonaws.com"
               ]
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "organizations:EnableAWSServiceAccess",
            "organizations:ListDelegatedAdministrators",
            "organizations:RegisterDelegatedAdministrator",
            "organizations:DeregisterDelegatedAdministrator"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "organizations:ServicePrincipal":[
                  "fms.amazonaws.com"
               ]
            }
         }
      }
   ]
}
```

Questa policy include le seguenti autorizzazioni:

- `fms:*`:

  Consente di lavorare con AWS Firewall Manager le risorse.

- `waf:*`, `waf-regional:*`:

  Consente di lavorare con AWS WAF le politiche.

- `elasticloadbalancing:SetWebACL`:

  Consente di associare elenchi di controllo degli accessi Web (ACL) a Elastic Load Balancers.

- `firehose:ListDeliveryStreams`:

Consente di visualizzare i log. AWS WAF

- `organizations:DescribeAccount`, `organizations:DescribeOrganization`, `organizations:ListRoots`, `organizations:ListChildren`, `organizations:ListAccounts`, `organizations:ListAccountsForParent`, `organizations:ListOrganizationalUnitsForParent`:

  Ti consente di lavorare con AWS Organizations.

- `shield:GetSubscriptionState`:

  Consente di visualizzare lo stato dell'abbonamento a una AWS Shield politica.

- `route53resolver:ListFirewallRuleGroups`, `route53resolver:GetFirewallRuleGroup`:

  Consente di utilizzare i gruppi di regole Route 53 Private DNS for VPC in base a una policy Route 53 Private DNS for VPC.

- `wafv2:ListRuleGroups`, `wafv2:ListAvailableManagedRuleGroups`, `wafv2:CheckCapacity`, `wafv2:PutLoggingConfiguration`, `wafv2:ListAvailableManagedRuleGroupVersions`:

  Consente di lavorare con le politiche. AWS WAFV2

- `network-firewall:DescribeRuleGroup`, `network-firewall:DescribeRuleGroupMetadata`, `network-firewall:ListRuleGroups`:

  Consente di lavorare con AWS Network Firewall le politiche.

- `ec2:DescribeAvailabilityZones`:

  Consente di visualizzare le zone di disponibilità di una AWS Network Firewall politica.

- `ec2:DescribeRegions`:

  Consente di visualizzare la regione di una politica nella AWS Firewall Manager console.

- `s3:GetBucketPolicy`:

  Consente di ottenere la policy sui bucket di Amazon S3 per i log. AWS WAF

- `ListDelegatedAdministrators`:

  Consente di elencare gli amministratori delegati di Amazon OpenSearch Service.

AWS politica gestita: FMS ServiceRolePolicy

Questa politica consente di AWS Firewall Manager gestire AWS le risorse per conto dell'utente in Firewall Manager e nei servizi integrati. Questa policy è attribuita al ruolo collegato ai servizi `AWSServiceRoleForFMS`. Per ulteriori informazioni sul ruolo collegato al servizio, consulta Utilizzo di ruoli collegati ai servizi per Firewall Manager.

Per i dettagli delle policy, consulta la console IAM di FMS ServiceRolePolicy.

AWS politica gestita: AWSFMAdminReadOnlyAccess

Garantisce l'accesso in sola lettura a tutte le risorse di AWS Firewall Manager.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "fms:Get*",
            "fms:List*",
            "waf:Get*",
            "waf:List*",
            "waf-regional:Get*",
            "waf-regional:List*",
            "firehose:ListDeliveryStreams",
            "organizations:DescribeOrganization",
            "organizations:DescribeAccount",
            "organizations:ListRoots",
            "organizations:ListChildren",
            "organizations:ListAccounts",
            "organizations:ListAccountsForParent",
            "organizations:ListOrganizationalUnitsForParent",
            "shield:GetSubscriptionState",
            "route53resolver:ListFirewallRuleGroups",
            "route53resolver:GetFirewallRuleGroup",
            "wafv2:ListRuleGroups",
            "wafv2:ListAvailableManagedRuleGroups",
            "wafv2:CheckCapacity",
            "wafv2:ListAvailableManagedRuleGroupVersions",
            "network-firewall:DescribeRuleGroup",
            "network-firewall:DescribeRuleGroupMetadata",
            "network-firewall:ListRuleGroups",
```

```
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeRegions"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetBucketPolicy"
         ],
         "Resource":[
            "arn:aws:s3:::aws-waf-logs-*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "organizations:ListDelegatedAdministrators"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "organizations:ServicePrincipal":[
                  "fms.amazonaws.com"
               ]
            }
         }
      }
   ]
}
```

Questa policy include le seguenti autorizzazioni:

- `fms:*`:

  Consente di visualizzare le risorse. AWS Firewall Manager
- `waf:Get*`, `waf-regional:Get*`:

  Consente di ottenere AWS WAF le politiche.
- `waf:List*`, `waf-regional:List*`:

  Consente di elencare AWS WAF le politiche.

- `firehose:ListDeliveryStreams`:

  Consente di elencare AWS WAF i log.

- `organizations:DescribeOrganization`, `organizations:DescribeAccount`, `organizations:DescribeOrganization`, `organizations:ListRoots`, `organizations:ListChildren`, `organizations:ListAccounts`, `organizations:ListAccountsForParent`, `organizations:ListOrganizationalUnitsForParent`:

  Consente di visualizzare AWS le risorse di Organizations.

- `shield:GetSubscriptionState`:

  Consente di visualizzare lo stato dell'abbonamento a una AWS Shield politica.

- `route53resolver:ListFirewallRuleGroups`, `route53resolver:GetFirewallRuleGroup`:

  Consente di ottenere ed elencare i gruppi di regole Route 53 Private DNS for VPC in una policy Route 53 Private DNS for VPC.

- `wafv2:ListRuleGroups`, `wafv2:ListAvailableManagedRuleGroups`, `wafv2:CheckCapacity`, `wafv2:ListAvailableManagedRuleGroupVersions`:

  Consente di elencare i gruppi di AWS WAFV2 regole, i gruppi di regole AWS Managed Rules nelle AWS WAFV2 politiche, la capacità dei gruppi di AWS WAFV2 regole e le versioni dei gruppi di regole AWS WAFV2 AWS Managed Rules.

- `network-firewall:DescribeRuleGroup`, `network-firewall:DescribeRuleGroupMetadata`, `network-firewall:ListRuleGroups`:

  Consente di visualizzare i gruppi di AWS Network Firewall regole e i metadati dei gruppi di regole.

- `ec2:DescribeAvailabilityZones`:

  Consente di visualizzare le zone di disponibilità di una AWS Network Firewall politica.

- `ec2:DescribeRegions`:

  Consente di visualizzare la regione di una politica nella AWS Firewall Manager console.

- `s3:GetBucketPolicy`:

  Consente di ottenere la policy sui bucket di Amazon S3 per i log. AWS WAF

- `ListDelegatedAdministrators`:

Consente di elencare gli amministratori delegati in. AWS Organizations

AWS politica gestita: AWSFMMemberReadOnlyAccess

Garantisce l'accesso in sola lettura alle risorse dei membri. AWS Firewall Manager Per i dettagli delle policy, consulta la console IAM all'indirizzo. AWSFMMemberReadOnlyAccess

Aggiornamenti di Firewall Manager alle policy AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Firewall Manager da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei documenti di Firewall Manager all'indirizzo. Cronologia dei documenti

Modifica	Descrizione	Data
FMS ServiceRolePolicy — Politica aggiornata	Sono state aggiunte autorizza zioni che consentono a Firewall Manager di descriver e se le AWS Config regole specificate sono conformi. Consulta la policy aggiornat a nella console IAM: FMS. ServiceRolePolicy	21 aprile 2023
FMSServiceRolePolicy: politica aggiornata	Sono state aggiunte autorizza zioni che consentono a Firewall Manager di descriver e gli attributi dell'istanza e dell'interfaccia di rete di Amazon EC2.	15 novembre 2022

Modifica	Descrizione	Data
	Consulta la policy aggiornat a nella console IAM: FMS. ServiceRolePolicy	
AWSFMAdminReadOnly Access— Politica aggiornata	Sono state aggiunte le autorizzazioni per il supporto AWS WAFV2, Shield, Network Firewall, DNS Firewall, gruppo di sicurezza Amazon VPC e policy. Vedi la policy aggiornata nella console IAM:. AWSFMAdmi nReadOnlyAccess	02 novembre 2022
AWSFMAdminFullAccess— Politica aggiornata	Sono state aggiunte le autorizzazioni per il supporto AWS WAFV2, Shield, Network Firewall, DNS Firewall, gruppo di sicurezza Amazon VPC e policy. Autorizzazioni Amazon SNS rimosse. Consulta la policy aggiornat a nella console IAM:. AWSFMAdminFullAccess	21 ottobre 2022
`FMSServiceRolePolicy` - Nuove autorizzazioni per le politiche firewall AWS Firewall Manager di terze parti	Questa modifica consente a Firewall Manager di creare ed eliminare gli endpoint VPC di Amazon EC2 associati a una policy firewall di terze parti.	30 marzo 2022

Modifica	Descrizione	Data
`FMSServiceRolePolicy` — Nuove autorizzazioni per le politiche AWS Network Firewall	Sono state aggiunte nuove autorizzazioni per supportare l'implementazione di firewall per le politiche del Network Firewall. Le nuove autorizzazioni consentono il recupero di informazioni sulle zone di disponibilità per gli account che rientrano nell'ambito di una politica.	16 febbraio 2022
`FMSServiceRolePolicy` — Nuove autorizzazioni per le politiche AWS Shield	Aggiunte nuove autorizzazioni per recuperare i tag per le risorse AWS WAF regionali e AWS WAF globali. Sono state aggiunte autorizzazioni AWS WAF regionali per recuperare gli ACL Web utilizzando un ARN di risorse. Sono state aggiunte le autorizzazioni per supportare la mitigazione automatica degli attacchi DDoS a livello di applicazione Shield.	07 gennaio 2022
`FMSServiceRolePolicy` — Nuove autorizzazioni per le politiche AWS Shield	È stata aggiunta una nuova autorizzazione per recuperare i tag per le risorse Elastic Load Balancing.	18 novembre 2021

Modifica	Descrizione	Data
`FMSServiceRolePolicy` — Nuove autorizzazioni per i gruppi di sicurezza e le politiche AWS Network Firewall	Sono state aggiunte nuove autorizzazioni per abilitare la registrazione centralizzata delle politiche. AWS Network Firewall Inoltre, sono state aggiunte autorizzazioni Amazon EC2 di sola lettura per supportare le modifiche al servizio Config che influiscono no AWS Firewall Manager sul modo in cui le risorse vengono interrogate per le policy dei gruppi di sicurezza.	29 settembre 2021
`FMSServiceRolePolicy` — Formati ARN per le risorse AWS WAF	Aggiornato il `FMSServiceRolePolicy` per standardizzare i formati AWS WAF ARN per le risorse. I formati ARN aggiornati sono `arn:aws:waf:*:*:*` e. `arn:aws:waf-regional:*:*:*`	12 agosto 2021
`FMSServiceRolePolicy` — Regioni aggiuntive in Cina	AWS Firewall Manager è abilitato `FMSServiceRolePolicy` per le regioni BJS e ZHY in Cina.	12 agosto 2021

Modifica	Descrizione	Data
`FMSServiceRolePolicy` — Aggiornamento alla politica esistente	Aggiunte nuove autorizzazioni per consentire AWS Firewall Manager la gestione del firewall Amazon Route 53 Resolver DNS. Questa modifica consente a Firewall Manager di configurare le associazioni Amazon Route 53 Resolver DNS Firewall. Ciò ti consente di utilizzare Firewall Manager per fornire protezioni DNS Firewall per i tuoi VPC in tutta l'organizzazione in. AWS Organizations	17 marzo 2021
Firewall Manager ha iniziato a tracciare le modifiche	Firewall Manager ha iniziato a tenere traccia delle modifiche per le politiche AWS gestite.	02 marzo 2021

Risoluzione dei problemi di AWS Firewall Manager identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Firewall Manager e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in Firewall Manager
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse di Firewall Manager

Non sono autorizzato a eseguire un'azione in Firewall Manager

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `fms:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fms:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `fms:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di passare un ruolo a Firewall Manager.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Firewall Manager. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse di Firewall Manager

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Firewall Manager supporta queste funzionalità, vedereCome AWS Shield funziona con IAM.
- Per scoprire come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Utilizzo di ruoli collegati ai servizi per Firewall Manager

AWS Firewall Manager utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a Firewall Manager. I ruoli collegati ai servizi sono predefiniti da Firewall Manager e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per conto dell'utente.

Un ruolo collegato al servizio semplifica la configurazione di Firewall Manager perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Firewall Manager definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo Firewall Manager può assumerne i ruoli. Le autorizzazioni definite includono policy di attendibilità e di autorizzazioni. Questa policy delle autorizzazioni non può essere collegata ad alcun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. In questo modo si proteggono le risorse del Firewall Manager perché non è possibile rimuovere inavvertitamente l'autorizzazione all'accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per Firewall Manager

AWS Firewall Manager utilizza il nome del ruolo collegato al servizio AWSServiceRoleForFMS per consentire a Firewall Manager di chiamare AWS i servizi per conto dell'utente per la gestione delle politiche del firewall e delle risorse dell' AWS Organizations account. Questa policy è allegata al ruolo AWS gestito. `AWSServiceRoleForFMS` Per ulteriori informazioni sul ruolo gestito, vedereAWS politica gestita: FMS ServiceRolePolicy.

Il ruolo AWSServiceRoleForFMS collegato al servizio si fida del servizio da assumere il ruolo. `fms.amazonaws.com`

La politica di autorizzazione dei ruoli consente a Firewall Manager di completare le seguenti azioni sulle risorse specificate:

- `waf`- Gestisci gli ACL Web AWS WAF classici, le autorizzazioni per i gruppi di regole e le associazioni degli ACL Web nel tuo account.
- `ec2`- Gestisci i gruppi di sicurezza su interfacce di rete elastiche e istanze Amazon EC2.
- `vpc`- Gestisci sottoreti, tabelle di routing, tag ed endpoint in Amazon VPC.
- `wafv2`- Gestisci gli ACL AWS WAF Web, le autorizzazioni per i gruppi di regole e le associazioni degli ACL Web nel tuo account.
- `cloudfront`- Crea ACL web per proteggere le distribuzioni. CloudFront
- `config`- Gestisci le AWS Config regole di proprietà di Firewall Manager nel tuo account.
- `iam`- Gestisci questo ruolo collegato al servizio e crea ruoli obbligatori e collegati al servizio AWS WAF Shield se configuri la registrazione e le politiche Shield. AWS WAF
- `organization`- Creare un ruolo collegato ai servizi di proprietà di Firewall Manager per gestire AWS Organizations le risorse utilizzate da Firewall Manager.
- `shield`- Gestisci le AWS Shield protezioni e le configurazioni di mitigazione L7 per le risorse del tuo account.

- `ram`- Gestisci la condivisione AWS RAM delle risorse per i gruppi di regole DNS Firewall e i gruppi di regole Network Firewall.
- `network-firewall`- Gestisci le risorse di proprietà di Firewall Manager e AWS Network Firewall le risorse Amazon VPC dipendenti nel tuo account.
- `route53resolver`- Gestisci le associazioni DNS Firewall di proprietà di Firewall Manager nel tuo account.

Consulta la policy completa nella console IAM: FMS. ServiceRolePolicy

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Firewall Manager

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando abiliti l'accesso a Firewall Manager o effettui AWS Management Console una `PutLoggingConfiguration` richiesta nell'interfaccia della riga di comando di Firewall Manager o nell'API Firewall Manager, Firewall Manager crea automaticamente il ruolo collegato al servizio.

È necessario disporre dell'autorizzazione `iam:CreateServiceLinkedRole` per attivare la registrazione.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando abiliti la registrazione di Firewall Manager, Firewall Manager crea nuovamente il ruolo collegato al servizio per te.

Modifica di un ruolo collegato ai servizi per Firewall Manager

Firewall Manager non consente di modificare il ruolo AWSServiceRoleForFMS collegato al servizio. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Firewall Manager

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non

utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

> **Note**
>
> Se il servizio Firewall Manager utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare il ruolo collegato al servizio utilizzando IAM

Utilizza la console IAM, la CLI IAM o l'API IAM per eliminare il ruolo collegato al AWSServiceRoleForFMS servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi di Firewall Manager

Firewall Manager supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, vedere Endpoint e quote di Firewall Manager.

Prevenzione del problema "confused deputy" tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel frattempo AWS, l'impersonificazione tra servizi può causare il problema del vicedirettore confuso. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Si consiglia di utilizzare `aws:SourceArn`le chiavi di contesto della condizione `aws:SourceAccount`globale nelle politiche delle risorse per limitare le autorizzazioni che AWS Firewall Manager forniscono un altro servizio alla risorsa. Utilizza `aws:SourceArn` se desideri consentire l'associazione di una sola risorsa all'accesso tra servizi. Utilizza `aws:SourceAccount` se desideri consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi.

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn`con l'ARN completo della risorsa. Se non conosci l'ARN completo della risorsa o scegli più risorse, utilizza la chiave di contesto della condizione globale `aws:SourceArn` con caratteri jolly (`*`) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:fms:*:`*`account-id`*`:*`.

Se il valore `aws:SourceArn` non contiene l'ID account, ad esempio un ARN di un bucket Amazon S3, è necessario utilizzare entrambe le chiavi di contesto delle condizioni globali per limitare le autorizzazioni.

Il valore di `aws:SourceArn` deve essere l' AWS account dell' AWS Firewall Manager amministratore.

Gli esempi seguenti mostrano come utilizzare la chiave di contesto della condizione `aws:SourceArn` globale in Firewall Manager per evitare il problema del confuso vice.

L'esempio seguente mostra come prevenire il problema del confuso vice utilizzando la chiave `aws:SourceArn` global condition context nella politica di attendibilità del ruolo Firewall Manager. Sostituisci *`Region`* e *`account-id`* con le tue informazioni.

```
{
  "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"
      }
    }
  }
}
```

Registrazione e monitoraggio in Firewall Manager

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Firewall Manager e delle tue AWS soluzioni. È necessario raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. AWS fornisce diversi strumenti per monitorare le risorse del Firewall Manager e rispondere a potenziali eventi:

CloudWatch Allarmi Amazon

Utilizzando gli CloudWatch allarmi, controlli una singola metrica per un periodo di tempo specificato. Se la metrica supera una determinata soglia, CloudWatch invia una notifica a un argomento o una policy di Amazon SNS. AWS Auto Scaling Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch.

AWS CloudTrail Registri

CloudTrail fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Firewall Manager. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a Firewall Manager, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi. Per ulteriori informazioni, consulta Registrazione delle chiamate API di AWS CloudTrail con.

Convalida della conformità per Firewall Manager

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

  > **Note**
  >
  > Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e

verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.

- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente AWS l'utilizzo per semplificare la gestione dei rischi e la conformità alle normative e agli standard di settore.

Resilienza in Firewall Manager

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

Sicurezza dell'infrastruttura nell' AWS Firewall Manager

In quanto servizio gestito, AWS Firewall Manager è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Si utilizzano chiamate API AWS pubblicate per accedere a Firewall Manager attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

AWS Firewall Manager quote

AWS Firewall Manager è soggetto alle seguenti quote (precedentemente denominate limiti).

AWS Firewall Manager ha quote predefinite che potresti aumentare e quote fisse.

Le policy dei gruppi di sicurezza gestite da Firewall Manager sono soggette alle quote standard di Amazon VPC. Per ulteriori informazioni, consulta Amazon VPC Quotas nella Amazon VPC User Guide.

Ogni politica Firewall Manager Network Firewall crea un firewall di rete con una politica firewall associata e i relativi gruppi di regole. Queste risorse Network Firewall sono soggette alle quote elencate nella sezione AWS Network Firewall quote nella Network Firewall Developer Guide.

Quote flessibili

AWS Firewall Manager prevede quote predefinite sul numero di entità per regione. È possibile richiedere un aumento di queste quote.

Tutti i tipi di policy

Risorsa	Quota predefinita per regione
Account per organizzazione in AWS Organizations	Può variare. Un invito inviato a un account rientra nel calcolo di questa quota. Il conteggio viene annullato se l'account invitato rifiuta, l'account di gestione annulla l'invito o l'invito scade.
Criteri di Firewall Manager per organizzazione in AWS Organizations.	50. Le specifiche e `Global` della regione `US East (N. Virginia)`

Risorsa	Quota predefinita per regione
	`Region` si riferiscono alla stessa regione, pertanto questo limite si applica al totale delle politiche combinate per entrambe.
Unità organizzative nell'ambito della politica di Firewall Manager.	20
Account che rientrano nell'ambito di una politica di Firewall Manager se si includono ed escludono esplicitamente singoli account.	200
Account che rientrano nell'ambito di una politica di Firewall Manager se non si includono o si escludono esplicitamente singoli account.	2.500
Tag che includono o escludono risorse in base alla politica di Firewall Manager.	8
Numero massimo di set di risorse per account.	20
Numero massimo di risorse per set di risorse.	100
Numero massimo di set di risorse per policy di Firewall Manager.	5

Policy di gruppo di sicurezza comuni

Risorsa	Quota predefinita per regione.
Gruppi di sicurezza primari per policy.	3
Istanze Amazon VPC nell'ambito della policy per account, inclusi i VPC condivisi.	100

Policy di gruppo di sicurezza del controllo dei contenuti

Risorsa	Quota predefinita per regione
Verifica i gruppi di sicurezza per policy.	1
Applicazioni per elenco di applicazioni.	50
Elenchi di applicazioni gestite personalizzate per le regole che consenton o tutto il traffico.	1
Elenchi di applicazioni gestite personalizzati in base alle regole delle policy.	1
Elenchi di applicazioni gestite personalizzate per account.	10
Protocolli per elenco di protocolli.	5
Elenchi di protocolli gestiti personalizzati per qualsiasi impostazione di una politica.	1
Elenchi di protocolli gestiti personalizzati per account.	10

AWS WAF politiche

Risorsa	Quota predefinita per regione
AWS WAF gruppi di regole per account amministratore di Firewall Manager.	100
AWS WAF Gruppi di regole classici per account amministratore di Firewall Manager.	10
Gruppi di regole per AWS WAF policy.	50

Politiche del firewall DNS

Risorsa	Quota predefinita per regione
Gruppi di regole DNS Firewall per policy Firewall Manager.	2

Quote rigide

Le seguenti quote per regione relative a non AWS Firewall Manager possono essere modificate.

Tutti i tipi di policy

Risorsa	Quota per regione
Il numero massimo di amministratori di Firewall Manager che è possibile avere in un' AWS Organizations organizzazione. È necessario avere un amministratore predefinito e fino a nove amministratori di Firewall Manager aggiuntivi.	10

Politiche del Network Firewall

Risorsa	Quota per regione
Numero di VPC a cui è possibile porre rimedio automaticamente per una singola policy.	1.000
Il numero di CIDR IPV4 che è possibile fornire per una singola policy.	50

Politiche di controllo dei contenuti dei gruppi di sicurezza

Risorsa	Quota per regione
Firewall Manager ha gestito elenchi di applicazioni per qualsiasi impostazione di una policy.	1
Firewall Manager ha gestito gli elenchi dei protocolli per qualsiasi impostazione di una policy.	1

AWS WAF politiche

Risorsa	Quota per regione
Unità di capacità ACL Web (WCU) totali per i gruppi di regole in una policy AWS WAF .	5.000

AWS WAF Politiche classiche

Risorsa	Quota per regione
AWS WAF Gruppi di regole classici per politica.	2:1 gruppo di regole creato dal cliente e 1 gruppo di Marketplace AWS regole.
AWS WAF Regole classiche per gruppo di regole Firewall Manager AWS WAF Classic.	10

AWS Firewall Manager Monitoraggio AWS WAF e AWS Shield Advanced

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni dei servizi.

> **Note**
>
> Per informazioni sul monitoraggio delle risorse Shield Advanced e sull'identificazione di possibili eventi DDoS utilizzando Shield Advanced, vedereAWS Shield.

Quando si inizia a monitorare questi servizi, è opportuno creare un piano di monitoraggio che includa le risposte alle seguenti domande:

- Quali sono gli obiettivi del monitoraggio?
- Di quali risorse si intende eseguire il monitoraggio?
- Con quale frequenza sarà eseguito il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio verranno utilizzati?
- Chi eseguirà i processi di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

La fase successiva consiste nello stabilire una baseline per le prestazioni normali di nell'ambiente, misurando le prestazioni in diversi momenti e con condizioni di carico differenti. Durante il monitoraggio AWS WAF, Firewall Manager, Shield Advanced e i servizi correlati archiviano i dati di monitoraggio cronologici in modo da poterli confrontare con i dati sulle prestazioni correnti, identificare i modelli di prestazioni normali e le anomalie delle prestazioni e ideare metodi per risolvere i problemi.

In effetti AWS WAF, è necessario monitorare almeno i seguenti elementi per stabilire una linea di base:

- Il numero di richieste Web consentite
- Il numero di richieste Web bloccate

Argomenti

Strumenti di monitoraggio

AWS fornisce vari strumenti che è possibile utilizzare per monitorare AWS WAF e AWS Shield Advanced. Alcuni di questi strumenti possono essere configurati in modo che eseguano il monitoraggio, mentre altri richiedono l'intervento manuale. Si consiglia di automatizzare il più possibile i processi di monitoraggio.

Strumenti di monitoraggio automatici

È possibile utilizzare i seguenti strumenti di monitoraggio automatizzato per osservare AWS WAF AWS Shield Advanced e segnalare quando qualcosa non va:

- Dashboard di panoramica sul traffico ACL Web: accedi ai riepiloghi del traffico Web valutato da un ACL Web accedendo alla pagina dell'ACL Web nella AWS WAF console e aprendo la scheda Panoramica del traffico.

  Le dashboard di panoramica del traffico forniscono riepiloghi quasi in tempo reale delle CloudWatch metriche di Amazon AWS WAF raccolte durante la valutazione del traffico web dell'applicazione. Puoi visualizzare i riepiloghi di tutto il tuo traffico web e del traffico valutato dai gruppi di regole di mitigazione intelligente delle minacce.

  Per ulteriori informazioni, consulta Dashboard di panoramica sul traffico ACL Web o accedi ai dashboard della console.
- Amazon CloudWatch Alarms: monitora una singola metrica in un periodo di tempo specificato ed esegui una o più azioni in base al valore della metrica rispetto a una determinata soglia in diversi periodi di tempo. L'operazione è una notifica inviata a un topic Amazon Simple Notification Service (Amazon SNS) o alla policy di Dimensionamento automatico Amazon EC2. Gli allarmi richiamano azioni solo per cambiamenti di stato sostenuti. CloudWatch gli allarmi non richiameranno azioni semplicemente perché si trovano in uno stato particolare; lo stato deve essere cambiato e mantenuto per un determinato numero di periodi. Per ulteriori informazioni, consulta Monitoraggio CloudFront dell'attività utilizzando. CloudWatch

> **Note**
>
> CloudWatch le metriche e gli allarmi non sono abilitati per. AWS Firewall Manager

Non solo puoi utilizzarle CloudWatch per monitorare AWS WAF e Shield Advanced come descritto inMonitoraggio con Amazon CloudWatch, ma dovresti utilizzarle anche per CloudWatch monitorare l'attività delle tue risorse protette. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Monitoraggio delle CloudFront attività CloudWatch nell'Amazon CloudFront Developer Guide
- Registrazione e monitoraggio in Amazon API Gateway nella API Gateway Developer Guide
- CloudWatch Metriche per il tuo Application Load Balancer nella Guida per l'utente di Elastic Load Balancing
- Monitoraggio e registrazione nella Guida per gli sviluppatori AWS AppSync
- Registrazione e monitoraggio in Amazon Cognito nella Amazon Cognito Developer Guide
- Visualizzazione dei log di App Runner trasmessi in streaming a CloudWatch Logs e visualizzazione dei parametri del servizio App Runner riportati nella Developer Guide CloudWatch AWS App Runner

- Amazon CloudWatch Logs: monitora, archivia e accedi ai tuoi file di registro da AWS CloudTrail o altre fonti. Per ulteriori informazioni, consulta What is Amazon CloudWatch Logs? .
- Amazon CloudWatch Events: automatizza i tuoi AWS servizi e rispondi automaticamente agli eventi di sistema. Gli eventi generati dai AWS servizi vengono forniti a CloudWatch Events quasi in tempo reale e puoi specificare azioni automatiche da intraprendere quando un evento corrisponde a una regola che hai scritto. Per ulteriori informazioni, consulta Che cos'è Amazon CloudWatch Events?
- AWS CloudTrail Monitoraggio dei log: condividi i file di CloudTrail registro tra account, monitora i file di registro in tempo reale inviandoli a CloudWatch Logs, scrivi applicazioni di elaborazione dei log in Java e verifica che i file di registro non siano cambiati dopo la consegna da parte di. CloudTrail Per ulteriori informazioni, consulta la sezione Registrazione delle chiamate API di AWS CloudTrail con Lavorare con i file di CloudTrail registro nella Guida per l'utente.AWS CloudTrail
- AWS Config— Visualizza la configurazione delle AWS risorse nel tuo AWS account, incluso il modo in cui le risorse sono correlate tra loro e come erano configurate in passato, in modo da poter vedere come le configurazioni e le relazioni cambiano nel tempo.

Strumenti di monitoraggio manuali

Un'altra parte importante del monitoraggio AWS WAF AWS Shield Advanced riguarda il monitoraggio manuale degli elementi non coperti dagli CloudWatch allarmi. Puoi visualizzare le AWS Management Console dashboard AWS WAF, Shield Advanced e altre per vedere lo stato del tuo AWS ambiente. CloudWatch Ti consigliamo di controllare anche i file di registro degli ACL e delle regole web.

- Ad esempio, per visualizzare la AWS WAF dashboard:
  - Nella scheda Richieste della pagina AWS WAF Web ACL, visualizza un grafico delle richieste totali e delle richieste che corrispondono a ciascuna regola che hai creato. Per ulteriori informazioni, consulta Visualizzazione di un esempio di richieste Web.
- Visualizza la CloudWatch home page per quanto segue:
  - Stato e allarmi attuali
  - Grafici degli allarmi e delle risorse
  - Stato di integrità dei servizi

  Inoltre, è possibile utilizzare CloudWatch per effettuare le seguenti operazioni:
  - Crea pannelli di controllo personalizzati per monitorare i servizi rilevanti.
  - Crea grafici dei dati dei parametri per la risoluzione di problemi e il rilevamento di tendenze.
  - Cerca e sfoglia tutte le metriche delle tue AWS risorse.
  - Crea e modifica gli allarmi per ricevere le notifiche dei problemi.

Monitoraggio con Amazon CloudWatch

Puoi monitorare le richieste Web, gli ACL e le regole Web utilizzando Amazon CloudWatch, che raccoglie ed elabora i dati grezzi da AWS WAF e AWS Shield Advanced in metriche leggibili quasi in tempo reale. Puoi utilizzare le statistiche in Amazon CloudWatch per avere una prospettiva sulle prestazioni della tua applicazione o del tuo servizio web. Per ulteriori informazioni, consulta Cosa c'è CloudWatch nella Amazon CloudWatch User Guide.

> **Note**
>
> CloudWatch le metriche e gli allarmi non sono abilitati per Firewall Manager.

Puoi creare un CloudWatch allarme Amazon che invia un messaggio Amazon SNS quando l'allarme cambia stato. Un allarme monitora un singolo parametro per un periodo di tempo specificato ed esegue una o più operazioni in base alla relazione tra il valore del parametro e una soglia impostata, su più intervalli predefiniti. L'operazione corrisponde all'invio di una notifica a un argomento di Amazon SNS o a una policy di Auto Scaling. Gli allarmi richiamano azioni solo per cambiamenti di stato sostenuti. CloudWatch gli allarmi non richiamano azioni semplicemente perché si trovano in uno stato particolare; lo stato deve essere cambiato e mantenuto per un determinato numero di periodi.

Argomenti

Visualizzazione di parametri e dimensioni

Le metriche vengono raggruppate prima in base allo spazio dei nomi del servizio e quindi in base alle varie combinazioni di dimensioni all'interno di ogni spazio dei nomi. AWS Firewall Manager non registra le metriche.

- Il AWS WAF namespace è `AWS/WAFV2`
- Lo spazio dei nomi Shield Advanced è `AWS/DDoSProtection`

> **Note**
>
> AWS WAF riporta le metriche una volta al minuto.
> Shield Advanced riporta le metriche una volta al minuto durante un evento e meno frequentemente altre volte.

Utilizza le seguenti procedure per visualizzare le metriche per AWS WAF e. AWS Shield Advanced

Per visualizzare le metriche utilizzando la console CloudWatch

1. Accedi AWS Management Console e apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.

2. Se necessario, cambia la regione con quella in cui si trovano le AWS risorse. Per CloudFront, scegli la regione Stati Uniti orientali (Virginia settentrionale).
3. Nel riquadro di navigazione, in Metriche, scegli Tutte le metriche, quindi cerca il servizio nella scheda Sfoglia.

Per visualizzare le metriche utilizzando la CLI AWS

- Per AWS/WAFV2, al prompt dei comandi usa il seguente comando:

  ```
  aws cloudwatch list-metrics --namespace "AWS/WAFV2"
  ```

  Per Shield Advanced, al prompt dei comandi usa il seguente comando:

  ```
  aws cloudwatch list-metrics --namespace "AWS/DDoSProtection"
  ```

AWS WAF metriche e dimensioni

AWS WAF riporta le metriche una volta al minuto. AWS WAF fornisce metriche e dimensioni nel namespace. `AWS/WAFV2`

Puoi visualizzare le informazioni di riepilogo relative alle AWS WAF metriche tramite la AWS WAF console, nella scheda Panoramica del traffico di Web ACL. Per ulteriori informazioni, vai alla console o consulta. Dashboard di panoramica sul traffico ACL Web

Puoi visualizzare le seguenti metriche per gli ACL Web, le regole, i gruppi di regole e le etichette.

- Le tue regole: le metriche sono raggruppate in base all'azione della regola. Ad esempio, quando si verifica una regola in Count modalità, le relative corrispondenze vengono elencate come `Count` metriche per l'ACL Web.
- I tuoi gruppi di regole: le metriche per i tuoi gruppi di regole sono elencate sotto le metriche dei gruppi di regole.
- Gruppi di regole di proprietà di un altro account: le metriche dei gruppi di regole sono generalmente visibili solo al proprietario del gruppo di regole. Tuttavia, se sovrascrivi l'azione della regola per una regola, le metriche relative a tale regola verranno elencate nelle metriche ACL Web. Inoltre, le etichette aggiunte da qualsiasi gruppo di regole sono elencate nelle metriche ACL Web

I gruppi di regole di questa categoria sonoAWS Regole gestite per AWS WAF, Marketplace AWS gruppi di regole gestitiGruppi di regole forniti da altri servizi, e i gruppi di regole condivisi con te da un altro account.

- Etichette: le etichette che sono state aggiunte a una richiesta Web durante la valutazione sono elencate nelle metriche delle etichette Web ACL. Puoi accedere alle metriche per tutte le etichette, indipendentemente dal fatto che siano state aggiunte dalle tue regole e dai tuoi gruppi di regole o dalle regole di un gruppo di regole di proprietà di un altro account.

Argomenti

Web ACL, gruppo di regole e metriche e dimensioni

Web ACL, gruppo di regole e metriche di regole

Parametro	Descrizione
`AllowedRequests`	Il numero di richieste Web consentite. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche valide: somma
`BlockedRequests`	Il numero di richieste Web bloccate. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche valide: somma
`CountedRequests`	Il numero di richieste Web contate. Criteri di segnalazione: vi è un valore diverso da zero.

Parametro	Descrizione
	Una richiesta Web contata è una richiesta che corrisponde ad almeno una delle regole. Il conteggio delle richieste viene solitamente utilizzato per i test. Statistiche valide: somma
`CaptchaRequests`	Il numero di richieste Web a cui sono stati applicati i controlli CAPTCHA. Criteri di segnalazione: vi è un valore diverso da zero. Una richiesta web CAPTCHA corrisponde a una regola con un'impostazione di azione. CAPTCHA Questa metrica registra tutte le richieste corrispon denti, indipendentemente dal fatto che abbiano un token CAPTCHA valido. Statistiche valide: somma
`RequestsWithValidCaptchaTok en`	Il numero di richieste Web a cui erano applicati i controlli CAPTCHA e che avevano un token CAPTCHA valido. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche valide: somma
`CaptchasAttempted`	Il numero di soluzioni inviate da un utente finale in risposta a un rompicapo CAPTCHA. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche valide: somma

Parametro	Descrizione
`CaptchasSolved`	Il numero di soluzioni di puzzle CAPTCHA presentate che hanno risolto con successo il puzzle. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche valide: somma
`ChallengeRequests`	Il numero di richieste Web a cui sono stati applicati i controlli di verifica. Criteri di segnalazione: vi è un valore diverso da zero. Una richiesta web di sfida corrisponde a una regola con un'impostazione di Challenge azione. Questa metrica registra tutte le richieste corrispondenti, indipendentemente dal fatto che abbiano un token di sfida valido. Statistiche valide: somma
`RequestsWithValidChallengeToken`	Il numero di richieste Web a cui sono stati applicati i controlli di verifica e che avevano un token di sfida valido. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche valide: somma

Parametro	Descrizione
`PassedRequests`	Il numero di richieste passate. Viene utilizzato solo per le richieste che vengono sottoposte a una valutazione del gruppo di regole senza corrispondere a nessuna delle regole del gruppo di regole. Criteri di segnalazione: vi è un valore diverso da zero. Le richieste passate sono richieste che non corrispon dono a nessuna delle regole del gruppo di regole. Statistiche valide: somma

ACL Web, gruppo di regole e dimensioni delle regole

Dimensione	Descrizione
`Region`	Obbligatorio per tutti i tipi di risorse protette ad eccezione delle CloudFront distribuzioni Amazon.
`Rule`	Una delle seguenti: • Il nome parametro di `Rule`. • ALL, che rappresenta tutte le regole all'interno di una WebACL o `RuleGroup` . • `Default_Action` (solo se combinato con la `WebACL` dimensione), che rappresenta l'azione assegnata a qualsiasi richiesta la cui valutazio ne non è stata interrotta dall'azione di una regola nell'ACL web.
`RuleGroup`	Il nome parametro di `RuleGroup` .
`WebACL`	Il nome parametro di `WebACL`.
`Country`	Il paese di origine della richiesta. Questa è la designazione a due caratteri dello standard 3166

Dimensione	Descrizione
	dell'Organizzazione internazionale per la standardizzazione (ISO). Ad esempio, USA per gli Stati Uniti e UA per l'Ucraina. Se una richiesta ha un'`X-Forwarded-For` intestazione, la AWS WAF utilizza per determinare questa impostazione. Altrimenti, AWS WAF utilizza il paese dell'IP del client. Questa determinazione è indipendente dalla logica utilizzata nelle regole per determinare il paese di origine. AWS WAF determina le posizioni degli IP utilizzando i database MaxMind GeoIP.
`Attack`	Il tipo di attacco AWS WAF identificato nella richiesta, in base alle regole e ai gruppi di regole utilizzati nell'ACL Web. Le tue regole e le regole dei gruppi di regole AWS gestite di base possono identificare i tipi di attacco. Ad esempio, le corrispondenze di regole Cross-Site Scripting (XSS) identificano i tipi di attacco XSS, mentre le regole basate sulla frequenza identificano i tipi di attacchi volumetrici. Il tipo di attacco indica in genere il tipo di regola che ha interrotto la valutazione della richiesta Web.
`Device`	Il tipo di dispositivo del client che ha inviato la richiesta, ottenuto dall'`user-agent` intestazione della richiesta Web.
`ManagedRuleGroup`	Il nome metrico del gruppo di regole gestito la cui regola ha interrotto la valutazione della richiesta Web.

Metriche e dimensioni delle etichette

Metriche per le etichette aggiunte alle richieste durante la valutazione in base alle tue regole e ai gruppi di regole gestiti che utilizzi nell'ACL web. Per informazioni, consulta Etichette sulle richieste web.

Per ogni singola richiesta web, AWS WAF memorizza le metriche per un massimo di 100 etichette. La tua valutazione ACL web può applicare più di 100 etichette e confrontarle con più di 100 etichette, ma solo le prime 100 vengono riportate nelle metriche.

Metriche delle etichette

Parametro	Descrizione
`AllowedRequests`	Il numero di etichette nelle richieste Web a cui è stata Allow applicata l'impostazione dell'azione. Le etichette possono essere state aggiunte in qualsiasi momento durante la valutazione della richiesta Web. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche valide: somma
`BlockedRequests`	Il numero di etichette nelle richieste Web a cui è stata Block applicata l'impostazione dell'azione. Le etichette possono essere state aggiunte in qualsiasi momento durante la valutazione della richiesta Web. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche valide: somma
`CountedRequests`	Il numero di etichette aggiunte alle richieste Web in base alle regole del gruppo di regole con un'impost azione di Count azione. Questa metrica è disponibile solo per il proprietario di un gruppo di regole, per le regole all'interno del gruppo di regole. In altri casi, le metriche dell'etic

Parametro	Descrizione
	hetta di conteggio vengono raggruppate nell'azione di terminazione applicata alla richiesta, ad esempio o. Allow Block Criteri di segnalazione: vi è un valore diverso da zero. Statistiche valide: somma
`CaptchaRequests`	Il numero di etichette sulle richieste Web a cui è stata applicata un'azione di terminazioneCAPTCHA. Le etichette possono essere state aggiunte in qualsiasi momento durante la valutazione della richiesta Web. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche valide: somma
`ChallengeRequests`	Il numero di etichette sulle richieste Web a cui è stata applicata un'azione di Challenge terminazione. Le etichette possono essere state aggiunte in qualsiasi momento durante la valutazione della richiesta Web. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche valide: somma

Dimensioni dell'etichetta

Dimensione	Descrizione
`Region`	Obbligatorio per tutti i tipi di risorse protette ad eccezione delle CloudFront distribuzioni Amazon.
`WebACL`	Il nome parametro di `WebACL`.

Dimensione	Descrizione
`RuleGroup`	Il nome parametro di `RuleGroup` . Utilizzato per la metrica`CountedRequests` .
`LabelNamespace`	Il prefisso dello spazio dei nomi dell'etichetta che è stata aggiunta alla richiesta.
`Label`	Il nome dell'etichetta che è stata aggiunta alla richiesta.
`Context`	Il gruppo di regole gestito che fungeva da contesto per l'aggiunta dell'etichetta. Ad esempio, il contesto per le etichette di gestione dei token, ad esempio il gruppo di regole AWS WAF gestite che utilizza la gestione dei token su richiesta, come il gruppo di regole gestito da Bot Control o ATP. `awswaf:managed:token:accepted` Questa dimensione non si applica a tutte le etichette.

Metriche e dimensioni di visibilità dei bot gratuite

Quando non utilizzi Bot Control nella tua ACL web, AWS WAF applica il gruppo di regole gestito da Bot Control a un campione delle tue richieste web, senza costi aggiuntivi. Questo può darti un'idea del traffico bot che arriva alle tue risorse protette. Per informazioni su Bot Control, consultaAWS WAF Gruppo di regole Bot Control.

Metriche di visibilità dei bot gratuite

Parametro	Descrizione
`SampleAllowedRequest`	Il numero di richieste campionate che hanno un'Allowazione. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche valide: somma

Parametro	Descrizione
`SampleBlockedRequest`	Il numero di richieste campionate che hanno un'Blockazione. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche valide: somma
`SampleCaptchaRequest`	Il numero di richieste campionate che hanno un'CAPTCHAazione. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche valide: somma
`SampleChallengeRequest`	Il numero di richieste campionate che hanno un'Challengeazione. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche valide: somma
`SampleCountRequest`	Il numero di richieste campionate che hanno un'Countazione. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche valide: somma

Dimensioni di visibilità dei bot gratuite

Dimensione	Descrizione
`Region`	Obbligatorio per tutti i tipi di risorse protette ad eccezione delle CloudFront distribuzioni Amazon.

Dimensione	Descrizione
`WebACL`	Il nome parametro di `WebACL`.
`BotCategory`	Il nome della categoria di bot rilevata, in base alle etichette delle richieste Web.
`VerificationStatus`	Il nome dello stato di verifica del bot rilevato, in base alle etichette delle richieste Web.
`Signal`	Il nome dei segnali del bot rilevati, in base alle etichette delle richieste Web.

AWS Shield Advanced metriche

Shield Advanced pubblica le metriche di CloudWatch rilevamento, mitigazione e principali contributori di Amazon per tutte le risorse che protegge. Queste metriche migliorano la tua capacità di monitorare le tue risorse rendendo possibile la creazione e la configurazione di CloudWatch dashboard e allarmi per esse.

La console Shield Advanced presenta riepiloghi di molte delle metriche registrate. Per informazioni, consulta Visibilità sugli eventi DDoS.

Se abiliti la mitigazione automatica degli attacchi DDoS a livello di applicazione per una protezione a livello di applicazione,

Posizioni di segnalazione metrica

Shield Advanced riporta le metriche nella regione Stati Uniti orientali (Virginia settentrionale), `us-east-1` per quanto segue:

- I servizi globali Amazon CloudFront e Amazon Route 53.
- Gruppi di protezione. Per informazioni sui gruppi di protezione, vedereAWS Shield Advanced gruppi di protezione.

Per altri tipi di risorse, Shield Advanced riporta le metriche nella regione della risorsa.

Tempistica della rendicontazione delle metriche

Shield Advanced riporta i parametri ad Amazon CloudWatch su una AWS risorsa più frequentemente durante gli eventi DDoS rispetto a quando non è in corso alcun evento. Shield Advanced riporta le metriche una volta al minuto durante un evento e poi una volta subito dopo la fine dell'evento.

Sebbene non sia in corso alcun evento, Shield Advanced riporta le metriche una volta al giorno, all'ora assegnata alla risorsa. Questo rapporto periodico mantiene le metriche attive e disponibili per l'uso in allarmi e dashboard personalizzati CloudWatch .

Consigli sugli allarmi

Ti consigliamo di creare allarmi per avvisarti di circostanze che richiedono attenzione. Come punto di partenza, puoi creare un allarme per ogni risorsa protetta che segnala quando la metrica di `DDoSDetected` rilevamento è diversa da zero. Un valore diverso da zero in questa metrica non implica necessariamente che sia in corso un attacco DDoS, ma consigliamo di esaminare più da vicino lo stato della risorsa quando la metrica si trova in questo stato.

In caso di inondazioni di richieste, ti consigliamo di creare allarmi per controlli compositi che tengano conto anche di fattori come lo stato delle applicazioni e il volume delle richieste web. Puoi scegliere di attivare un allarme in base alle altre tre metriche che segnalano il volume di traffico per varie dimensioni dei vettori di attacco. Considerando la capacità dell'applicazione e avvisando quando il traffico si avvicina alle limitazioni dell'applicazione, è possibile creare una serie di regole che avvisano l'utente quando necessario, senza troppi rumori indesiderati.

Argomenti

Metriche di rilevamento

Shield Advanced fornisce le metriche e le dimensioni nel `AWS/DDoSProtection` namespace.

Metriche di rilevamento

Parametro	Descrizione
`DDoSDetected`	Indica se è in corso un evento DDoS per un determinato Amazon Resource Name (ARN).

Parametro	Descrizione
	Questa metrica ha un valore diverso da zero durante un evento.
DDoSAttackBitsPerSecond	Il numero di bit osservati durante un evento DDoS per un determinato Amazon Resource Name (ARN). Questa metrica è disponibile solo per gli eventi DDoS di rete e trasporto (livello 3 e livello 4). Questa metrica ha un valore diverso da zero durante un evento. Unità: bit
DDoSAttackPacketsPerSecond	Il numero di pacchetti osservati durante un evento DDoS per un determinato Amazon Resource Name (ARN). Questa metrica è disponibile solo per gli eventi DDoS di rete e trasporto (livello 3 e livello 4). Questa metrica ha un valore diverso da zero durante un evento. Unità: pacchetti
DDoSAttackRequestsPerSecond	Il numero di richieste osservate durante un evento DDoS per un determinato Amazon Resource Name (ARN). Questo parametro è disponibile solo per gli eventi DDoS di livello 7. Il parametro è segnalato solo per gli eventi di livello 7 più significativi. Questa metrica ha un valore diverso da zero durante un evento. Unità: richieste

Shield Advanced pubblica la `DDoSDetected` metrica senza altre dimensioni. Le metriche di rilevamento rimanenti includono le `AttackVector` dimensioni che corrispondono al tipo di attacco, dal seguente elenco:

- `ACKFlood`
- `ChargenReflection`
- `DNSReflection`
- `GenericUDPReflection`
- `MemcachedReflection`
- `MSSQLReflection`
- `NetBIOSReflection`
- `NTPReflection`
- `PortMapper`
- `RequestFlood`
- `RIPReflection`
- `SNMPReflection`
- `SSDPReflection`
- `SYNFlood`
- `UDPFragment`
- `UDPTraffic`
- `UDPReflection`

Metriche di mitigazione

Shield Advanced fornisce metriche e dimensioni nel `AWS/DDoSProtection` namespace.

Metriche di mitigazione

Parametro	Descrizione
`VolumePacketsPerSecond`	Il numero di pacchetti al secondo che sono stati eliminati o passati da una mitigazione implementata in risposta a un evento rilevato. Unità: pacchetti

Dimensioni di mitigazione

Dimensione	Descrizione
`ResourceArn`	Nome della risorsa Amazon (ARN)
`MitigationAction`	Il risultato di una mitigazione applicata. I valori possibili sono `Pass` o `Drop`.

Principali metriche dei contributori

Shield Advanced fornisce metriche nel `AWS/DDoSProtection` namespace.

Principali metriche dei contributori

Parametro	Descrizione
`VolumePacketsPerSecond`	Il numero di pacchetti al secondo per un collaboratore principale. Unità: pacchetti
`VolumeBitsPerSecond`	Il numero di bit al secondo per un collaboratore principale. Unità: bit

Shield Advanced pubblica le metriche dei principali contributori in base alle combinazioni di dimensioni che caratterizzano i contributori dell'evento. Puoi utilizzare una delle seguenti combinazioni di dimensioni per tutte le metriche dei principali contributori:

- `ResourceArn`, `Protocol`
- `ResourceArn`, `Protocol`, `SourcePort`
- `ResourceArn`, `Protocol`, `DestinationPort`
- `ResourceArn`, `Protocol`, `SourceIp`
- `ResourceArn`, `Protocol`, `SourceAsn`
- `ResourceArn`, `TcpFlags`

Dimensioni dei principali contributori

Dimensione	Descrizione
`ResourceArn`	Amazon Resource Name (ARN).
`Protocol`	Nome del protocollo IP, `TCP` oppure`UDP`.
`SourcePort`	Porta TCP o UDP di origine.
`DestinationPort`	Porta TCP o UDP di destinazione.
`SourceIp`	Indirizzo IP di origine.
`SourceAsn`	Numero di sistema autonomo (ASN) di origine.
`TcpFlags`	Combinazione di flag presenti in un pacchetto TCP, separati da un trattino (). `-` I flag monitorati sono,,. `ACK` `FIN` `RST` `SYN` Questo valore di dimensione viene sempre visualizzato in ordine alfabetico. For example: `ACK-FIN-RST-SYN` , `ACK-SYN` e `FIN-RST`.

AWS Firewall Manager notifiche

AWS Firewall Manager non registra i parametri, quindi non puoi creare CloudWatch allarmi Amazon specifici per Firewall Manager. Tuttavia, puoi configurare le notifiche di Amazon SNS per avvisarti di potenziali attacchi. Per creare notifiche Amazon SNS in Firewall Manager, consulta. Fase 4: Configurazione delle notifiche e degli allarmi Amazon SNS CloudWatch

Registrazione delle chiamate API di AWS CloudTrail con

AWS WAF e AWS Firewall Manager sono integrati con AWS CloudTrail un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio. AWS Shield Advanced CloudTrail acquisisce un sottoinsieme di chiamate API per questi servizi come eventi, incluse le chiamate dalle console AWS WAF Shield Advanced o Firewall Manager e le chiamate di codice alle API, AWS WAF Shield Advanced o Firewall Manager. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi events for, AWS WAF Shield Advanced o Firewall

Manager. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a questi servizi, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

Per ulteriori informazioni CloudTrail, incluso come configurarlo e abilitarlo, consulta la Guida per l'AWS CloudTrail utente.

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività di evento supportata in AWS WAF, Shield Advanced o Firewall Manager, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella Cronologia eventi. Puoi visualizzare, cercare e scaricare eventi recenti in Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo Account AWS, inclusi gli eventi per AWS WAF, Shield Advanced o Firewall Manager, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail si applica a tutte le regioni. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un trail
- CloudTrail Servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

AWS WAF informazioni in AWS CloudTrail

Tutte AWS WAF le azioni vengono registrate AWS CloudTrail e documentate nell'AWS WAF API Reference. Ad esempio, chiamate e `DeleteWebACL` generano voci nei file di CloudTrail registro. `ListWebACL` `UpdateWebACL`

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali dell'utente root

- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio

Per ulteriori informazioni, vedete CloudTrailUserIdentity Element.

Esempio: voci dei file di AWS WAF registro

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. AWS CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta da un'fonte e include informazioni sull'azione richiesta, data e ora dell'azione, parametri richiesti e così via. CloudTrail i file di registro non sono una traccia ordinata delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Di seguito sono riportati alcuni esempi di voci di CloudTrail registro per le operazioni ACL AWS WAF Web.

Esempio: voce di CloudTrail registro per `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"
}
```

Esempio: voce di CloudTrail registro per `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"
}
```

Esempio: voce di CloudTrail registro per `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"
}
```

Esempio: voce di CloudTrail registro per `DeleteWebACL`

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/sheqiang-Isengard",
    "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"
}
```

Esempio: voci AWS WAF classiche dei file di registro

AWS WAF Classic è la versione precedente di AWS WAF. Per informazioni, consulta AWS WAF Classico.

La voce di log dimostra le operazioni `CreateRule`, `GetRule`, `UpdateRule` e `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 informazioni in CloudTrail

AWS Shield Advanced supporta la registrazione delle seguenti azioni come eventi nei file di CloudTrail registro:

- ListAttacks
- DescribeAttack
- CreateProtection
- DescribeProtection
- DeleteProtection
- ListProtections
- CreateSubscription
- DescribeSubscription
- GetSubscriptionState

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali dell'utente root
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, vedete l'elemento CloudTrail userIdentity.

Esempio: voci dei file di registro Shield Advanced

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra le azioni `DeleteProtection` e `ListProtections`.


```
[
 {
   "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 informazioni in CloudTrail

AWS Firewall Manager supporta la registrazione delle seguenti azioni come eventi nei file di CloudTrail registro:

- AssociateAdminAccount
- DeleteNotificationChannel

- DeletePolicy
- DisassociateAdminAccount
- PutNotificationChannel
- PutPolicy
- GetAdminAccount
- GetComplianceDetail
- GetNotificationChannel
- GetPolicy
- ListComplianceStatus
- ListPolicies

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali dell'utente root
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, vedete l'elemento CloudTrail userIdentity.

Esempio: voci del file di registro di Firewall Manager

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'azione `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"
    }
```

Utilizzo dell' AWS Shield Advanced API AWS WAF and

Questa sezione descrive come effettuare richieste all'API Shield Advanced per la AWS WAF creazione e la gestione di match set, regole e ACL Web, AWS WAF nonché l'abbonamento e le protezioni in Shield Advanced. Questa sezione ti farà prendere confidenza con i componenti delle richieste, il contenuto delle risposte e le modalità di autenticazione delle richieste.

Argomenti

Utilizzo degli AWS SDK

Se utilizzi un linguaggio che AWS fornisce un SDK, utilizza l'SDK anziché cercare di utilizzare le API a modo tuo. Gli SDK semplificano l'autenticazione, si integrano facilmente con l'ambiente di sviluppo e forniscono un facile accesso ai comandi AWS WAF Shield Advanced. Per ulteriori informazioni sugli AWS SDK, consulta Download degli strumenti l'argomento. Configurazione

Effettuare richieste HTTPS a AWS WAF o Shield Advanced

AWS WAF e le richieste Shield Advanced sono richieste HTTPS, come definito da RFC 2616. Come qualsiasi richiesta HTTP, una richiesta a AWS WAF o Shield Advanced contiene un metodo di richiesta, un URI, intestazioni di richiesta e un corpo della richiesta. La risposta contiene un codice di stato HTTP, intestazioni di risposta e talvolta un corpo di risposta.

URI di richiesta

L'URI della richiesta è sempre una barra singola, `/`.

Intestazioni HTTP

AWS WAF e Shield Advanced richiedono le seguenti informazioni nell'intestazione di una richiesta HTTP:

Host (obbligatorio)

L'endpoint che specifica dove vengono create le tue risorse. Per informazioni sugli endpoint, consulta AWS Service Endpoints. Ad esempio, il valore dell'`Host`intestazione AWS WAF per una CloudFront distribuzione è. `waf.amazonaws.com:443`

x-amz-date o Data (obbligatorio)

La data utilizzata per creare la firma contenuta nell'intestazione `Authorization`. La data va specificata nel formato ISO 8601 standard, in UTC, come nell'esempio seguente:

```
x-amz-date: 20151007T174952Z
```

È necessario includere `x-amz-date` o `Date`. (Alcune biblioteche di client HTTP non consentono di impostare l'intestazione `Date`). Quando è presente un'`x-amz-date`intestazione, AWS WAF ignora qualsiasi `Date` intestazione durante l'autenticazione della richiesta.

Il timestamp deve essere compreso tra 15 minuti e l'ora del AWS sistema in cui viene ricevuta la richiesta. In caso contrario, il tentativo di richiesta fallisce con il codice di errore `RequestExpired` per evitare che qualcun altro ripeta la tua richiesta.

Autorizzazione (Obbligatoria)

Le informazioni necessarie per l'autenticazione della richiesta. Per ulteriori informazioni sulla creazione di questa intestazione, consulta Autenticazione di richieste.

X-Amz-Target (Obbligatorio)

Una sequenza di `AWSWAF_` o `AWSShield_`, la versione API senza punteggiatura, un punto (`.`) e il nome dell'operazione, ad esempio:

`AWSWAF_20150824.CreateWebACL`

Content-Type (Condizionale)

Specifica che il tipo di contenuto è JSON e la versione di JSON, come nell'esempio seguente:

```
Content-Type: application/x-amz-json-1.1
```

Condizione: obbligatoria per le `POST` richieste.

Content-Length (Condizionale)

La lunghezza del messaggio (senza le intestazioni) secondo la specifica RFC 2616.

Condizione: necessaria se il corpo della richiesta contiene informazioni (la maggior parte dei kit di strumenti aggiunge automaticamente questa intestazione).

Quello che segue è un esempio di intestazione per una richiesta HTTP per la creazione di un ACL Web su 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
```

Corpo della richiesta HTTP

Molte azioni dell'API AWS WAF and Shield Advanced richiedono l'inclusione di dati in formato JSON nel corpo della richiesta.

La seguente richiesta di esempio utilizza una semplice istruzione JSON per aggiornare e includere l'indirizzo IP 192.0.2.44 (`IPSet`rappresentato nella notazione CIDR come 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"
         }
      }
   ]
}
```

Risposte HTTP

Le azioni API All AWS WAF e Shield Advanced includono dati in formato JSON nella risposta.

Si elencano di seguito alcune intestazioni importanti nella risposta HTTP e il modo in cui vanno gestite nella tua applicazione, se possibile:

HTTP/1.1

Questa intestazione è seguita da un codice di stato. Il codice di stato 200 indica un'operazione riuscita.

- Tipo: stringa

x-amzn- RequestId

Un valore creato da AWS WAF o Shield Advanced che identifica in modo univoco la tua richiesta, ad esempio,. `K2QH8DN0U907N97FNA2GDLL80BVV4KQNSO5AEMVJF66Q9ASUAAJG` Se hai un problema con AWS WAF, AWS puoi usare questo valore per risolvere il problema.

- Tipo: stringa

Content-Length

La lunghezza in byte del corpo della risposta.

- Tipo: stringa

Data

La data e l'ora in cui AWS WAF Shield Advanced ha risposto, ad esempio mercoledì 7 ottobre 2015 12:00:00 GMT.

- Tipo: stringa

Risposte agli errori

Se una richiesta genera un errore, la risposta HTTP contiene i seguenti valori:

- Un documento di errore in JSON come corpo della risposta
- Content-Type
- Il codice di stato HTTP 3xx, 4xx o 5xx applicabile

Di seguito è illustrato un esempio di documento di errore in 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"}
```

Autenticazione di richieste

Se utilizzi un linguaggio che AWS fornisce un SDK per, ti consigliamo di utilizzare l'SDK. Tutti gli AWS SDK semplificano notevolmente il processo di firma delle richieste e consentono di risparmiare una notevole quantità di tempo rispetto all'utilizzo della AWS WAF nostra API Shield Advanced. In più, gli SDK si integrano senza difficoltà nel tuo ambiente di sviluppo e ti offrono semplice accesso ai comandi correlati.

AWS WAF e Shield Advanced richiedono l'autenticazione di ogni richiesta inviata firmando la richiesta. Per firmare una richiesta, devi calcolare una firma digitale utilizzando una funzione hash crittografica, che restituisce un valore hash basato sull'input. L'input include il testo della richiesta e la

tua chiave di accesso segreta. La funzione hash restituisce un valore hash che includi nella richiesta come firma. La firma è parte dell'intestazione `Authorization` della richiesta.

Dopo aver ricevuto la richiesta, AWS WAF Shield Advanced ricalcola la firma utilizzando la stessa funzione di hash e lo stesso input utilizzati per firmare la richiesta. Se la firma risultante corrisponde alla firma nella richiesta, AWS WAF Shield Advanced elabora la richiesta. In caso contrario, la richiesta viene rifiutata.

AWS WAF e Shield Advanced supporta l'autenticazione tramite AWS Signature Version 4. La procedura per il calcolo di una firma può essere suddivisa in tre fasi:

Fase 1. Creazione di una richiesta canonica

Crea la richiesta HTTP in formato canonico come descritto in Fase 1: creazione di una richiesta canonica per Signature Version 4 nella guida Riferimenti generali di Amazon Web Services.

Fase 2: creazione di una stringa di firma

Crea una stringa che utilizzerai come uno dei valori di input per la funzione hash crittografica. La stringa, denominata la stringa di firma, è una sequenza dei seguenti valori:

- Nome dell'algoritmo hash
- Data richiesta
- Stringa di ambito credenziali
- Richiesta in formato canonico creata durante la fase precedente

La stringa di ambito credenziali è anch'essa una concatenazione di data, regione e informazioni sul servizio.

Per il parametro `X-Amz-Credential`, è necessario specificare quanto segue:

- Il codice per l'endpoint al quale stai inviando la richiesta: `us-east-2`.
- `waf` per l'abbreviazione del servizio.

Per esempio:

```
X-Amz-Credential=AKIAIOSFODNN7EXAMPLE/20130501/us-east-2/waf/
aws4_request
```

Fase 3. Creazione di una firma

Crea una firma per la richiesta utilizzando una funzione hash crittografica che accetta due stringhe di input:

- La tua stringa di firma, creata durante la Fase 2
- Una chiave derivata La chiave derivata viene calcolata a partire dalla tua Secret Access Key e utilizzando la stringa di ambito credenziali per creare una serie di codici HMAC (Hashed Message Authentication Code).

Informazioni correlate

Le seguenti risorse correlate possono rivelarsi utili durante l'utilizzo di questo servizio.

Le seguenti risorse sono disponibili per AWS WAF AWS Shield Advanced, e AWS Firewall Manager.

- Linee guida per l'implementazione AWS WAF: pubblicazione tecnica con le raccomandazioni attuali per l'implementazione AWS WAF per proteggere le applicazioni Web nuove e esistenti.
- AWS forum di discussione: forum basato sulla community per discutere di questioni tecniche relative a questo e ad altri servizi. AWS
- AWS WAF Forum di discussione: un forum basato sulla community in cui gli sviluppatori possono discutere di questioni tecniche relative a. AWS WAF
- Shield Advanced Discussion Forum: un forum basato sulla community in cui gli sviluppatori possono discutere di questioni tecniche relative a Shield Advanced.
- AWS WAF informazioni sul prodotto: la pagina web principale per informazioni su funzionalità AWS WAF, prezzi e altro ancora.
- Informazioni sul prodotto Shield Advanced: la pagina Web principale per informazioni su Shield Advanced, incluse funzionalità, prezzi e altro ancora.

Le seguenti risorse sono disponibili per Amazon Web Services.

- Corsi e workshop: collegamenti a corsi specializzati e basati su ruoli, oltre a laboratori di autoapprendimento per aiutarti ad affinare le tue abilità e acquisire esperienza pratica. AWS
- AWS Developer Center: esplora i tutorial, scarica strumenti e scopri gli eventi per sviluppatori. AWS
- AWS Strumenti per sviluppatori: collegamenti a strumenti di sviluppo, SDK, toolkit IDE e strumenti a riga di comando per lo sviluppo e la gestione di applicazioni. AWS
- Centro risorse introduttivo: scopri come configurare Account AWS, entrare a far parte della AWS community e lanciare la tua prima applicazione.
- Tutorial pratici: segui i tutorial per avviare la step-by-step tua prima applicazione su. AWS
- AWS Whitepaper: collegamenti a un elenco completo di AWS white paper tecnici, su argomenti quali architettura, sicurezza ed economia e redatti da Solutions Architects o altri esperti tecnici. AWS

- AWS Support Center: l'hub per la creazione e la gestione dei casi. AWS Support Include anche collegamenti ad altre risorse utili, come forum, domande frequenti tecniche, stato di salute del servizio e AWS Trusted Advisor.
- AWS Support— La pagina web principale per informazioni su AWS Support one-on-one, un canale di supporto a risposta rapida per aiutarti a creare ed eseguire applicazioni nel cloud.
- Contatti - Un punto di contatto centrale per richieste relative a fatturazione, account, eventi, uso illecito e altre questioni relative ad AWS .
- AWS Termini del sito: informazioni dettagliate sul nostro copyright e marchio, sull'account, sulla licenza e sull'accesso al sito e altri argomenti.

Cronologia dei documenti

Questa pagina elenca le modifiche significative a questa documentazione.

Le funzionalità del servizio a volte vengono implementate in modo incrementale nelle AWS regioni in cui il servizio è disponibile. Aggiorniamo questa documentazione solo per la prima versione. Non forniamo informazioni sulla disponibilità delle regioni e non annunciamo implementazioni successive delle regioni. Per informazioni sulla disponibilità regionale delle funzionalità del servizio e per iscriverti alle notifiche sugli aggiornamenti, vedi Cosa c'è di AWS nuovo? .

Modifica	Descrizione	Data
Aggiornamenti per le politiche dei gruppi di sicurezza di Firewall Manager	Abbiamo aggiornato le nostre politiche dei gruppi di sicurezza per il controllo dell'utilizzo e migliorato la documentazione. Consulta la sezione sulla politica di controllo dell'utilizzo e le sezioni sulle migliori pratiche e limitazioni.	2 aprile 2024
Esempi aggiornati di Bot Control	Sono stati aggiunti esempi che illustrano il livello di ispezione mirato ed esempi esistenti aggiornati per rispecchiare le migliori pratiche.	27 marzo 2024
Esempi ATP aggiornati	È stato aggiunto un esempio che illustra la configurazione dell'ispezione della risposta e sono stati aggiornati gli esempi esistenti per rispecchiare le migliori pratiche.	27 marzo 2024

Esempi ACFP aggiornati	È stato aggiunto un esempio che illustra la configurazione dell'ispezione della risposta.	27 marzo 2024
Aggiorna i limiti del flusso CloudWatch di log di Amazon Logs	AWS WAF non prevede più limiti ACL per Web alla pubblicazione dei log nei flussi di log di Logs. CloudWatch	27 marzo 2024
AWS Shield Advanced protezioni a livello di applicazione (livello 7)	Linee guida generali e di best practice aggiornate per il rilevamento e la mitigazione a livello di applicazione, l'uso dell'ACL Web, le regole basate sulla frequenza e la mitigazione automatica degli attacchi DDoS a livello di applicazione.	14 marzo 2024
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento del gruppo di regole di reputazione IP.	13 marzo 2024
Modifiche ai limiti di dimensione delle ispezioni corporee	AWS WAF ora supporta limiti più elevati per le dimensioni delle ispezioni corporee per alcune risorse regionali.	7 marzo 2024
Finestra di valutazione configurabile per regole basate sulla tariffa AWS WAF	Ora puoi configurare la finestra temporale utilizzata dalle regole basate sulla tariffa per contare le richieste, portandola a 1, 2, 5 o 10 minuti. L'impostazione predefinita è 5, che era l'unica opzione prima di questa versione.	28 febbraio 2024

Informazioni di registrazione estese per e CAPTCHACh allenge	Il livello superiore `captchaResponse` e `challenge Response` i campi sono ora compilati con l'ultima di queste azioni da applicare a una richiesta, terminante o non terminante. In precedenza, questi campi venivano compilati solo per terminare le azioni.	22 febbraio 2024
JavaScript Gestione delle chiavi API CAPTCHA	Ora puoi eliminare le chiavi API CAPTCHA JS tramite le API. AWS WAF	6 febbraio 2024
AWS WAF Audio dei puzzle CAPTCHA	La versione audio del puzzle CAPTCHA ora supporta più lingue.	6 febbraio 2024
AWS WAF challenge ed etichettatura con token CAPTCHA	La gestione dei token ora aggiunge etichette per il token CAPTCHA e ha migliorato l'etichettatura dei token per il token di sfida.	20 dicembre 2023
Regole gestite aggiornate AWS per AWS WAF	AWS Managed Rules per l' AWS WAF aggiornamento del gruppo di regole noto per gli input errati.	16 dicembre 2023
Regole AWS gestite aggiornate per AWS WAF	AWS Managed Rules per l' AWS WAF aggiornamento del gruppo di regole noto per gli input errati.	14 dicembre 2023

Regole AWS gestite aggiornate per AWS WAF	AWS Managed Rules per l' AWS WAF aggiornamento del gruppo di regole principali (CRS).	6 dicembre 2023
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per i seguenti gruppi di regole AWS WAF aggiornati: AWS WAF Bot Control.	5 dicembre 2023
AWS Config Prerequisiti aggiornati di Firewall Manager	Se utilizzi un ruolo IAM personalizzato anziché il ruolo gestito di Firewall Manager per AWS Config, devi assicurarti che la tua politica di autorizzazione consenta al AWS Config registratore di registrare le risorse di Firewall Manager.	17 novembre 2023
AWS WAF dashboard della console	Abbiamo corretto la guida per la visualizzazione di tutte le regole e le richieste di esempio per un ACL Web nella console. AWS WAF	17 novembre 2023
Regole gestite aggiornate AWS per AWS WAF	AWS Managed Rules per l' AWS WAF aggiornamento del gruppo di regole Bot Control.	14 novembre 2023
AWS WAF la console dispone di nuovi dashboard ACL Web	La pagina Web ACL nella AWS WAF console dispone di nuovi dashboard per la panoramica del traffico Web.	14 novembre 2023

Gruppo di regole gestito ATP aggiornato	Informazioni corrette sull'etichetta per le regole `VolumetricIpFailedLoginResponseHigh` e. `VolumetricSessionFailedLoginResponseHigh`	13 novembre 2023
Gruppo di regole gestito ACFP aggiornato	Informazioni corrette sull'etichetta per le regole e. `VolumetricIPSuccessfulResponse` `VolumetricSessionSuccessfulResponse`	13 novembre 2023
Regole AWS gestite aggiornate per AWS WAF	AWS Managed Rules per l' AWS WAF aggiornamento del gruppo di regole principali (CRS).	2 novembre 2023
Mitigazione DDoS automatica a livello di applicazione Shield Advanced	Shield Advanced ora mantiene una regola basata sulla frequenza nel gruppo di regole di mitigazione automatica che limita il volume di richieste provenienti da indirizzi IP noti per essere fonti di attacchi DDoS.	31 ottobre 2023
Regole gestite aggiornate per AWSAWS WAF	AWS Managed Rules per l' AWS WAF aggiornamento del gruppo di regole principali (CRS).	30 ottobre 2023

Il gruppo di regole gestito da Bot Control ha rimosso l'etichetta del segnale per il CSP della richiesta	Il gruppo di regole gestito da Bot Control ha rimosso l'etichetta del segnale che indica il provider di servizi cloud (CSP).	28 ottobre 2023
Bot Control ha gestito l'etichetta del segnale del gruppo di regole per il CSP della richiesta	Le etichette dei segnali del gruppo di regole gestite da Bot Control includono un'etichetta che indica il provider di servizi cloud (CSP).	27 ottobre 2023
Informazioni aggiornate sulle autorizzazioni AWS WAF IAM	Per le AWS WAF azioni che gestiscono le associazioni ACL Web, la sezione delle azioni politiche elenca ora i requisiti di autorizzazione per ogni tipo di risorsa dell'applicazione Web.	25 ottobre 2023
Firewall Manager: gestione degli ACL Web modificati	Quando si abilita la gestione degli ACL Web non associati, Firewall Manager non include gli ACL Web modificati nella pulizia unica delle risorse non utilizzate.	19 ottobre 2023
Regole gestite aggiornate per AWSAWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento del gruppo di regole del sistema operativo POSIX,`AWSManagedRulesUnixRuleSet` .	12 ottobre 2023
AWS WAF metriche, dimensioni aggiunte	AWS WAF ha aggiunto nuove dimensioni per la visualizzazione delle metriche ACL Web.	12 ottobre 2023

Regole AWS gestite aggiornate per AWS WAF	AWS Managed Rules per l' AWS WAF aggiornamento del gruppo di regole principali (CRS).	11 ottobre 2023
Aggiornamento alle specifiche SDK AWS WAF per dispositivi mobili	È stata aggiunta l'`storeTokenInCookieStorage` operazione a. `WAFTokenProvider`	11 ottobre 2023
Distribuzioni di eccezioni Regole AWS gestite per AWS WAF	AWS Managed Rules for AWS WAF ha rilasciato due versioni statiche del gruppo di regole Known Bad Inputs e ha aggiornato la versione predefinita in modo che faccia riferimento alla versione statica più recente.	4 ottobre 2023
AWS WAF L'entità HTML decodifica la trasformazione del testo	Ha ampliato la funzionalità della trasformazione del testo di decodifica delle entità HTML.	4 ottobre 2023
Aggiunta una nuova opzione alla politica comune del gruppo di sicurezza Firewall Manager	Firewall Manager ora può distribuire i riferimenti ai gruppi di sicurezza ai gruppi di sicurezza di replica.	3 ottobre 2023
AWS WAF aggiunge l'ispezione dell'impronta digitale JA3	Ora puoi eseguire una corrispondenza esatta con l'impronta digitale JA3 della richiesta web.	26 settembre 2023

Aggiornamenti alle impostazioni delle regole dei criteri dei gruppi di sicurezza di Firewall Manager	Firewall Manager ora supporta il riferimento ai gruppi di sicurezza dai gruppi di sicurezza primari ai gruppi di sicurezza di replica.	25 settembre 2023
Attenuazione degli attacchi DDoS a livello di applicazione automatica Shield Advanced aggiornata	Firewall Manager ora supporta le risorse Application Load Balancer per le policy Shield Advanced configurate con la mitigazione automatica degli attacchi DDoS a livello di applicazione.	14 settembre 2023
Regole gestite aggiornate AWS per AWS WAF	AWS Regole gestite per i seguenti gruppi di regole AWS WAF aggiornati: AWS WAF Bot Control.	6 settembre 2023
AWS WAF Bot Control	Il livello di protezione mirato del gruppo di regole gestito da Bot Control ora verifica il riutilizzo dei token tra gli indirizzi IP. Ora fornisce anche un'analisi opzionale con apprendimento automatico delle statistiche sul traffico per rilevare alcune attività relative ai bot.	6 settembre 2023
Aggiornamento alle specifiche SDK per dispositivi mobili AWS WAF	Sono stati ridotti i valori min, max e default `tokenRefreshDelaySec` da min 300, max 600 e default 300 a min 88, max 300 e default 88.	5 settembre 2023

Regole AWS gestite aggiornate per AWS WAF	AWS Managed Rules per l' AWS WAF aggiornamento del gruppo di regole AWS WAF Bot Control.	30 agosto 2023
Mitigazione DDoS automatica a livello di applicazione Shield Advanced	Sono state aggiunte linee guida per l'utilizzo AWS CloudFormation per la gestione degli ACL Web utilizzati con la mitigazione automatica degli attacchi DDoS a livello di applicazione.	30 agosto 2023
Nuova opzione di policy di gruppo di sicurezza per il controllo dei contenuti di Firewall Manager	È stata aggiunta una nuova opzione per il controllo dei gruppi di regole eccessiva mente permissivi e una migliore descrizione delle procedure della console.	29 agosto 2023
Nuova opzione Firewall Manager Shield e AWS WAF policy	Se si abilita la gestione degli ACL Web non associati in and AWS WAF Shield, Firewall Manager crea ACL Web negli account rientranti nell'ambito delle policy solo se gli ACL Web verranno utilizzati da almeno una risorsa.	9 agosto 2023
Regole gestite aggiornate per AWSAWS WAF	AWS Managed Rules per l' AWS WAF aggiornamento del gruppo di regole principali (CRS).	26 luglio 2023

Aggregazione di regole basata sulla frequenza sul percorso URI	Ora puoi specificare il percorso URI nelle chiavi di aggregazione personalizzate per le regole basate sulla frequenza.	19 luglio 2023
Nuova opzione AWS WAF relativa alle regole politiche in AWS Firewall Manager	AWS Firewall Manager aggiunge il supporto per la configurazione dei limiti di dimensione dell'ispezione del corpo delle richieste AWS WAF Web.	18 luglio 2023
AWS WAF modifiche alle politiche gestite	Aggiornato `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` , e `AWSWAFConsoleReadOnlyAccess` per aggiungere l'accesso AWS verificato ai tipi di risorse con cui è possibile proteggersi AWS WAF.	17 giugno 2023
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per AWS WAF aggiungere il gruppo di regole`AWSManagedRulesACFPRuleSet` .	13 giugno 2023
Aggiornamento alla prevenzione dell'acquisizione di account AWS WAF Fraud Control (ATP)	È ora possibile specificare l'endpoint di accesso per il gruppo di regole gestito ATP utilizzando un'espressione regolare.	13 giugno 2023

Nuove informazioni per l'API CAPTCHA JavaScript	La nuova sezione descrive come creare un puzzle CAPTCHA personalizzato quando si AWS WAF risponde a una richiesta con un CAPTCHA.	13 giugno 2023
Nuovo gruppo di regole gestito da ACFP	Utilizza il nuovo gruppo di regole `AWSManagedRulesACFPRuleSet` per rilevare e bloccare i tentativi fraudolenti di creazione di account.	13 giugno 2023
Creazione AWS WAF di nuovi account Fraud Control e prevenzione delle frodi (ACFP)	Puoi rilevare e bloccare i tentativi fraudolenti di creazione di account con il nuovo gruppo di regole gestito per la prevenzione delle AWS WAF frodi sulla creazione di account Fraud Control (ACFP). `AWSManagedRulesACFPRuleSet` Con CloudFront le distribuzioni protette, puoi anche utilizzare ACFP per bloccare nuovi tentativi di creazione di account da parte di clienti che hanno recentemente inviato troppi tentativi di creazione di account falliti.	13 giugno 2023

AWS WAF modifiche alle politiche gestite	Aggiornato `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` , e `AWSWAFConsoleReadOnlyAccess` per correggere le impostazioni di accesso ai AWS App Runner servizi.	6 giugno 2023
Aggiunta una limitazione per le politiche dei gruppi di sicurezza di Firewall Manager	Se un VPC condiviso viene successivamente annullato , Firewall Manager non eliminerà i gruppi di sicurezza di replica nell'account associato.	2 giugno 2023
Nuovo componente di richiesta AWS WAF : Header order	Ora puoi confrontare con un elenco ordinato dei nomi delle intestazioni nella richiesta.	30 maggio 2023
Regole AWS gestite aggiornate per AWS WAF	Aggiornato il set di regole del sistema operativo Linux.	22 maggio 2023
È stata aggiornata l'organizzazione della sezione AWS WAF delle regole	Gli elenchi delle istruzioni sulle regole sono ora raggruppati per tipo di dichiarazione.	16 maggio 2023
Argomento spostato: Elenco degli indirizzi IP a velocità limitata	L'argomento relativo all'elenco degli indirizzi IP la cui velocità è limitata da una regola basata sulla velocità è ora incluso nell'argomento Regole basate sulla tariffa.	16 maggio 2023

Opzioni estese per le regole basate sulla tariffa	Ora puoi limitare la velocità delle richieste Web in base a chiavi di aggregazione diverse dagli indirizzi IP e puoi aggregarle utilizzando combinazioni di chiavi. Puoi anche limitare la velocità per tutte le richieste che corrispondono a un'istruzione scope-down, senza ulteriori aggregazioni.	16 maggio 2023
Aumento della quota di Firewall Manager	Il numero di policy di Firewall Manager per organizzazione è aumentato AWS Organizations da 20 a 50. Aumento del numero massimo di gruppi di sicurezza primari per policy da uno a tre. È stato modificato il numero massimo di WCU da una quota flessibile a una quota rigida.	5 maggio 2023
Aumento del numero massimo di WCU per gruppo di regole	Ora puoi utilizzare fino a 5.000 unità di capacità Web ACL (WCU) per gruppo di regole senza richiedere un aumento del supporto. Questo nuovo limite non può essere aumentato.	1 maggio 2023
AWS WAF Posizioni dei bucket di log di Amazon S3 con prefissi	AWS WAF ora consente i prefissi nei nomi dei bucket di log di Amazon S3.	1 maggio 2023

Regole gestite aggiornate per AWSAWS WAF	AWS Managed Rules per l' AWS WAF aggiornamento del gruppo di regole principali (CRS).	28 aprile 2023
È stato aggiunto il supporto per le istanze di accesso AWS verificato a AWS WAF	Ora puoi associare un ACL AWS WAF Web a un'istanz a di accesso verificato. Questa modifica è disponibi le solo nella versione più recente AWS WAF e non nella versione AWS WAF classica.	28 aprile 2023
Capitolo rivisto sull'utilizzo di più amministratori di Firewall Manager	Ora puoi designare più amministratori di Firewall Manager per creare e gestire le risorse firewall della tua organizzazione.	24 aprile 2023
AWS Firewall Manager aggiornamento gestito delle politiche	Aggiornato `FMSServiceRolePolicy` .	21 aprile 2023
Nuova integrazione delle applicazioni JavaScript client per CAPTCHA	Ora puoi personalizzare il posizionamento e le caratteri stiche del puzzle CAPTCHA nelle tue applicazioni client. JavaScript	20 aprile 2023

L'integrazione delle applicazioni è stata rinominata Intelligent Threat Integration	Abbiamo rinominato la funzionalità esistente per le integrazioni delle applicazioni client in integrazioni intelligenti contro le minacce, per aiutare a distinguere tra questa funzionalità e la nuova integrazione delle applicazioni CAPTCHA per. JavaScript	20 aprile 2023
Prezzi variabili per WCU Web ACL oltre 1.500	L'utilizzo di più di 1.500 unità di capacità Web ACL (WCU) nel Web ACL comporta costi aggiuntivi, che vengono adattati automaticamente all'aumento e alla diminuzione dell'utilizzo delle Web ACL WCU. L'ACL Web è al massimo di 5.000 WCU.	11 aprile 2023
Aumento del numero massimo di WCU per ACL web	Ora puoi utilizzare fino a 5.000 unità di capacità ACL Web (WCU) per ACL Web senza richiedere un aumento del supporto. Questo nuovo limite non può essere aumentato.	11 aprile 2023
Limiti di dimensione delle ispezioni corporee per gli ACL CloudFront web	Per gli ACL Web che proteggono CloudFront le distribuzioni Amazon, puoi aumentare il limite di dimensione dell'ispezione del corpo fino a 64 KB nella tua configurazione ACL Web.	11 aprile 2023

Aumento delle dimensioni delle ispezioni corporee per CloudFront	Il limite massimo di dimension e per le ispezioni AWS WAF corporee per CloudFront le distribuzioni Amazon è aumentato da 8 KB a 64 KB. Il limite di dimensione di ispezione predefinito per CloudFront è di 16 KB.	11 aprile 2023
Nuove opzioni relative alle regole AWS WAF politiche in AWS Firewall Manager	AWS Firewall Manager aggiunge il supporto per la prevenzione dell'acquisizione di account AWS WAF Fraud Control (ATP) e i gruppi di regole AWS gestite da AWS WAF Bot Control, le destinazi oni di registrazione di Amazon S3, le `CAPTCHA` sostituzioni delle regole e le azioni delle regole `Challenge` e gli elenchi di domini token.	7 aprile 2023
Firewall Manager supporta i bucket Amazon S3 come destinazioni di registrazione per la registrazione AWS WAF	Ora puoi utilizzare i bucket Amazon S3 come destinazi oni di registrazione nelle tue policy. AWS WAF	7 aprile 2023

AWS WAF modifiche alle politiche gestite	Aggiornato `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` , e `AWSWAFConsoleReadOnlyAccess` per aggiungere AWS App Runner servizi ai tipi di risorse con cui è possibile proteggersi AWS WAF.	30 marzo 2023
È stato aggiunto un avviso sull'utilizzo dei tag all'interno delle politiche dei gruppi di sicurezza	Firewall Manager non aggiornerà i tag dei gruppi di sicurezza esistenti né creerà nuovi gruppi di sicurezza se la politica contiene tag che sono in conflitto con la politica dei tag dell'organizzazione.	28 marzo 2023
Aggiornamento delle informazioni sul ruolo di servizio	Aggiornamento delle modalità di utilizzo di un ruolo di servizio con Firewall Manager.	8 marzo 2023
Informazioni corrette su come le regole basate sulla velocità eseguono la limitazione della velocità	Le regole basate sulla frequenza con istruzioni ridotte limitano solo le richieste con limite di frequenza che corrispondono all'istruzione scope-down della regola. Stavamo affermando che la limitazione si applicava a tutte le richieste per qualsiasi indirizzo IP a velocità limitata.	1 marzo 2023

Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento del gruppo di regole dell'applicazione PHP.	27 febbraio 2023
È stato aggiunto il supporto per AWS App RunnerAWS WAF	È ora possibile associare un ACL AWS WAF Web a un AWS App Runner servizio. Questa modifica è disponibile solo nella versione più recente AWS WAF e non nella versione AWS WAF classica.	23 febbraio 2023
È stata aggiornata la guida IAM per AWS Firewall Manager	Guida aggiornata per l'allineamento alle best practice IAM. Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.	16 febbraio 2023
Regole AWS gestite aggiornate per AWS WAF	AWS Managed Rules for AWS WAF ha aggiornato il gruppo di regole `AWSManagedRulesATPRuleSet` per aggiungere l'ispezione della risposta di accesso negli ACL Web che proteggono le CloudFront distribuzioni Amazon.	15 febbraio 2023
AWS WAF Controllo delle frodi e ispezione della risposta agli accessi (Account Takeover Prevention, ATP)	Per CloudFront le distribuzioni protette, ora puoi utilizzare ATP per bloccare nuovi tentativi di accesso da parte di client che hanno recentemente inviato troppi tentativi di accesso non riusciti.	15 febbraio 2023

Regole AWS gestite aggiornate per AWS WAF	Aggiornato il set di regole di base.	25 gennaio 2023
Le migliori pratiche per la mitigazione intelligente delle minacce	È stata aggiunta una sezione con le migliori pratiche per l'implementazione di Bot Control, ATP e altre funzionalità intelligenti di mitigazione delle minacce.	22 gennaio 2023
Come ispezionare gli pseudo header HTTP/2	È stata aggiunta una sezione che mappa le pseudo intestazioni HTTP/2 ai componenti di richiesta web corrispondenti.	20 gennaio 2023
È stata aggiornata la guida IAM per Classic AWS WAF	Guida aggiornata per l'allineamento alle best practice IAM. Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.	3 gennaio 2023
È stata aggiornata la guida IAM per AWS WAF	Guida aggiornata per l'allineamento alle best practice IAM. Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.	3 gennaio 2023
È stata aggiornata la guida IAM per AWS Shield	Guida aggiornata per l'allineamento alle best practice IAM. Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.	3 gennaio 2023
Aggiornamento delle politiche del firewall DNS di Amazon Route 53 Resolver	Sono state aggiunte informazioni sull'eliminazione dei gruppi di regole del firewall DNS di Amazon Route 53 Resolver.	29 dicembre 2022

Regole gestite aggiornate per AWSAWS WAF	Aggiornato il set di regole del sistema operativo Linux.	15 dicembre 2022
Regole AWS gestite aggiornate per AWS WAF	Aggiornato il set di regole di base.	5 dicembre 2022
Firewall Manager aggiunge il supporto per le politiche Fortigate Cloud Native Firewall (CNF) as a Service	Firewall Manager ora supporta le policy CNF di Fortigate.	2 dicembre 2022
AWS Config Requisito rimosso per le politiche DNS Firewall	Per le policy DNS Firewall, ora devi solo abilitare Config per il tipo di risorsa EC2 VPC.	17 novembre 2022
AWS Firewall Manager aggiornamento gestito delle politiche	Aggiornato `FMSServiceRolePolicy` .	15 novembre 2022
Espansione delle opzioni linguistiche per il puzzle AWS WAF CAPTCHA	Il puzzle CAPTCHA ora offre le sue istruzioni scritte in più lingue. Le istruzioni all'interno di ogni puzzle audio sono ancora fornite solo in inglese.	11 novembre 2022
Nuove quote Firewall Manager per set di risorse	Sono state aggiunte nuove quote per i set di risorse.	8 novembre 2022
Aggiunto il supporto per i set di risorse	È possibile creare set di risorse per raggruppare le risorse da gestire in una politica di Firewall Manager.	8 novembre 2022
Aggiungi il supporto per l'importazione di firewall da Network Firewall	È ora possibile importare e gestire i firewall esistenti nelle politiche Network Firewall utilizzando set di risorse.	8 novembre 2022

AWS Firewall Manager aggiornamento gestito delle politiche	Aggiornato `AWSFMAdminReadOnlyAccess` .	2 novembre 2022
La dichiarazione Geo Match ora aggiunge etichette alle richieste per paese e regione	Ora puoi gestire le origini delle richieste geografiche a livello di regione combinando la corrispondenza geografica con la corrispondenza delle etichette.	31 ottobre 2022
La sezione di primo livello è stata rinominata: Protezioni gestite	La sezione è ora denominata AWS WAF Intelligent Threat Mitigation, in linea con le nostre pagine di marketing.	27 ottobre 2022
Nuovo livello di protezione mirato nel gruppo di regole gestito da Bot Control	Il gruppo di regole gestito da Bot Control offre ora regole aggiuntive e mirate per il rilevamento e la mitigazione di bot sofisticati. Questo livello di protezione è disponibile a pagamento.	27 ottobre 2022
Nuova sezione sui AWS WAF token	Scopri come AWS WAF utilizza i token per la mitigazione intelligente delle minacce.	27 ottobre 2022
È stata aggiunta una nota importante sull'aggiornamento delle politiche del firewall di rete di Firewall Manager	Quando si aggiorna una policy di Firewall Manager, tutte le policy Network Firewall create dalla policy verranno aggiornate con la configurazione della policy Network Firewall della policy di Firewall Manager.	27 ottobre 2022

L'azione ha la precedenza nei gruppi di regole	È ora possibile sostituire le azioni delle regole in un gruppo di regole con qualsiasi impostazione di azione delle regole. Come per l'override dell'Countazione precedent e, è possibile applicare le sostituzioni a tutte le regole di un gruppo di regole e alle singole regole.	27 ottobre 2022
AWS WAF nuova opzione di Challenge azione delle regole	È possibile configurare le regole per utilizzare aChalleng e, per verificare che le richieste vengano inviate dai browser.	27 ottobre 2022
AWS WAF consente la condivisione di token tra più applicazioni protette	Puoi abilitare l'uso dei token su più applicazioni protette configurando un elenco di domini di token per il tuo ACL web.	27 ottobre 2022
La specifica di tutte le intestazioni non distingue tra maiuscole e minuscole	È stata modificata la specifica di tutte le intestazioni per non fare distinzione tra maiuscole e minuscole. Ciò corrispon de al comportamento dell'inte stazione singola.	26 ottobre 2022
AWS Firewall Manager modifiche alle politiche	È stato aggiornato l'elenco delle politiche per la concessio ne manuale dell'accesso completo alle AWS Firewall Manager risorse.	21 ottobre 2022

AWS Firewall Manager modifiche alle politiche gestite	Correzioni a. `AWSFMAdmi nFullAccess`	21 ottobre 2022
Regole AWS gestite aggiornate per AWS WAF	Aggiornato il gruppo di regole noto per gli input errati.	20 ottobre 2022
Regole AWS gestite aggiornate per AWS WAF	Aggiornato il gruppo di regole noto per gli input errati.	5 ottobre 2022
Aggiornamento alle specifiche SDK AWS WAF per dispositivi mobili	Il valore predefinito è stato abbassato `tokenRefr eshDelaySec` da 600 (10 minuti) a 300 (5 minuti).	30 settembre 2022
Regole AWS gestite aggiornate per AWS WAF	Sono stati corretti i nomi delle etichette forniti in questa documentazione per i seguenti gruppi di regole: sistema operativo POSIX, applicazione PHP, applicazione. WordPress	19 settembre 2022
Nuova opzione AWS WAF relativa alle regole politiche in AWS Firewall Manager	AWS Firewall Manager ora supporta richieste e risposte web personalizzate per le azioni web predefinite nelle AWS WAF politiche.	9 settembre 2022
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento dei seguenti gruppi di regole: Reputazione IP.	30 agosto 2022

AWS WAF modifiche alle politiche gestite	Aggiornato `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` , e `AWSWAFConsoleReadOnlyAccess` per aggiungere pool di utenti Amazon Cognito ai tipi di risorse con cui puoi proteggerti. AWS WAF	25 agosto 2022
AWS WAF Fraud Control e prevenzione dell'acquisizione di account (ATP)	Ora puoi utilizzare la funzionalità AWS WAF Fraud Control Account Takeover Prevention (ATP) con le distribuzioni Amazon CloudFront .	24 agosto 2022
Regole gestite aggiornate AWS per AWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento dei seguenti gruppi di regole: Input non validi noti.	22 agosto 2022
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per i seguenti gruppi di regole AWS WAF aggiornati:`AWSManagedRulesATPRuleSet` .	11 agosto 2022
È stato aggiunto il supporto per i pool di utenti di Amazon Cognito a AWS WAF	Ora puoi associare un ACL AWS WAF Web a un pool di utenti Amazon Cognito. Questa modifica è disponibile solo nell'ultima versione di AWS WAF e non nella AWS WAF versione classica.	11 agosto 2022

È stata aggiunta una sezione sulle distribuzioni per i gruppi di regole AWS Managed Rules con versioni diverse	È stata aggiunta una nuova sezione che documenta le distribuzioni per i gruppi di regole Managed Rules con versioni diverse. AWS La sezione include informazioni su come vengono denominat e le versioni predefinite durante le distribuzioni release candidate.	29 luglio 2022
Requisiti aggiornati per la configurazione della registraz ione per le politiche del Network Firewall	Sono stati aggiunti requisiti per le politiche di Network Firewall che utilizzano un bucket Amazon S3 crittogra fato come destinazione dei log.	26 luglio 2022
Opzione del livello di sensibili tà per l'istruzione della regola SQLi	È ora possibile aumentare la sensibilità delle istruzioni delle regole di iniezione SQL. Ciò non modifica il comportamento delle istruzioni esistenti, il cui livello di sensibilità è predefini to diLOW.	15 luglio 2022
Aggiunta l'opzione di configura zione della politica Network Firewall	Firewall Manager ora supporta l'ordine di valutazione stateful e le azioni predefinite nelle configurazioni delle policy firewall di Network Firewall.	14 luglio 2022
Aggiornamenti alle impostazi oni delle regole dei criteri dei gruppi di sicurezza di Firewall Manager	Firewall Manager ora supporta la distribuzione dei tag dai gruppi di sicurezza primari ai gruppi di sicurezza di replica.	7 luglio 2022

Aggiornamenti alla guida AWS Shield	Sono state ampliate le informazioni nella guida Shield per descrivere come Shield esegue la mitigazione degli eventi.	24 giugno 2022
Linee guida aggiornate per testare e ottimizzare le protezioni AWS WAF	La guida generale per il test e la messa a punto AWS WAF è stata aggiornata e ora è un argomento di primo livello.	20 giugno 2022
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per i seguenti gruppi di regole AWS WAF aggiornati: Core rule set (CRS).	9 giugno 2022
Il nuovo Firewall Manager ha confuso le linee guida sostitutive	Sono state aggiunte indicazioni su come prevenire il confuso problema secondario per Firewall Manager.	1 giugno 2022
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per i seguenti gruppi di regole AWS WAF aggiornati: Core rule set (CRS).	24 maggio 2022
Nuovi componenti della AWS WAF richiesta: Headers e Cookies	Ora puoi controllare i cookie in una richiesta web e puoi controllare tutte le intestazioni in una richiesta web, oltre a una sola intestazione.	29 aprile 2022

AWS WAF gestione di componenti oversize (body, header e cookie request)	Ora puoi AWS WAF specifica re come gestire i corpi di richiesta, le intestazioni e i cookie di grandi dimensioni all'interno delle tue regole che esaminano questi component i. Le regole che avete già creato per ispezionare questi componenti hanno un comportamento che corrispon de alla nuova Continue opzione per la gestione di sovradimensionamenti.	29 aprile 2022
AWS WAF Modifiche alle policy relative ai log di Amazon S3	Sono stati aggiornati la politica e l'esempio di autorizzazione dei log di Amazon S3.	12 aprile 2022
Opzione di mitigazione automatica degli attacchi DDoS a livello di applicazione ora disponibile con Application AWS Shield Advanced Load Balancer	Shield Advanced ora supporta la mitigazione automatica degli attacchi DDoS a livello di applicazione per Applicati on Load Balancer, rendendol a disponibile per tutte le protezioni a livello di applicazi one. È possibile configurare Shield Advanced per contare o bloccare automaticamente le richieste Web che fanno parte di un attacco DDoS a livello di applicazione su una risorsa protetta.	8 aprile 2022
È stato aggiunto un indicator e dell'impostazione della versione predefinita corrente per i gruppi di regole gestiti	Gli elenchi di versioni dei gruppi di regole gestiti ora indicano quale versione è quella predefinita corrente.	8 aprile 2022

Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per i seguenti gruppi di regole AWS WAF aggiornati: AWS WAF Bot Control.	6 aprile 2022
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento dei seguenti gruppi di regole: Input non validi noti.	31 marzo 2022
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento dei seguenti gruppi di regole: Input non validi noti.	30 marzo 2022
Firewall Manager aggiunge il supporto per Palo Alto Networks Cloud Next Generation Firewall (NGFW)	Firewall Manager ora supporta il Palo Alto Networks Cloud Next Generation Firewall (NGFW).	30 marzo 2022
Aggiungi il supporto per Palo Alto Networks Cloud NGFW a AWS Firewall Manager	AWS Firewall Manager ora supporta le politiche Palo Alto Networks Cloud Next Generation Firewall (NGFW).	30 marzo 2022
Aggiornamenti alla guida AWS Shield	Sono state ampliate le informazioni nella guida Shield per descrivere come Shield esegue il rilevamento degli eventi e per fornire esempi di architetture resilienti agli attacchi DDoS.	16 marzo 2022

Aggiornamenti alla guida AWS Shield	Ha ampliato le informazioni nella guida Shield e migliorato l'organizzazione di varie sezioni. Le principali modifiche riguardano le seguenti sezioni della guida Shield: supporto Shield Response Team (SRT), protezione delle risorse e visibilità negli AWS Shield Advanced eventi DDoS.	28 febbraio 2022
Firewall Manager ora supporta il modello di distribuzione centralizzato Network Firewall	È stata aggiunta una nuova procedura che spiega come configurare le politiche che utilizzano modelli di distribuzione distribuiti e centralizzati.	24 febbraio 2022
Firewall Manager aggiunge il supporto per il modello di distribuzione AWS Network Firewall centralizzato	Ora puoi configurare AWS Network Firewall le tue politiche per utilizzare il modello di distribuzione distribuito o centralizzato. Con il modello di distribuzione distribuito, Firewall Manager crea e gestisce gli endpoint firewall in ogni VPC che rientra nell'ambito della policy. Con il modello di implementazione centralizzato, Firewall Manager crea e mantiene gli endpoint firewall in un unico VPC di ispezione.	24 febbraio 2022

Aggiungi il supporto per il controllo delle versioni dei gruppi di regole AWS WAF gestiti a AWS Firewall Manager	AWS Firewall Manager ora supporta il controllo delle versioni dei gruppi di regole AWS WAF gestiti nelle AWS WAF politiche di Firewall Manager.	18 febbraio 2022
AWS Firewall Manager modifica gestita delle politiche	Aggiorna a `FMSServiceRolePolicy` .	16 febbraio 2022
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per i seguenti gruppi di regole AWS WAF aggiornati: elenchi di reputazione IP.	15 febbraio 2022
Regole AWS gestite aggiornate per AWS WAF	AWS Managed Rules for è AWS WAF stato aggiunto il gruppo di regole per la prevenzione dell'acquisizione di account AWS WAF Fraud Control (ATP). `AWSManagedRulesATPRuleSet`	11 febbraio 2022
Modifiche all'organizzazione della guida AWS WAF	È stata aggiunta una nuova sezione di primo livello per le protezioni gestite. È stata spostata la sezione CAPTCHA da Under rules a sotto la nuova sezione Managed Protections. È stata spostata la sezione delle etichette da under rules alla relativa sezione di primo livello.	11 febbraio 2022

AWS WAF integrazioni di applicazioni client	Utilizzate le API AWS WAF JavaScript e i client mobili per integrare le applicazioni client con i gruppi di regole AWS Managed Rules per la mitigazione intelligente delle minacce per un rilevamento avanzato.	11 febbraio 2022
AWS WAF Controllo delle frodi e prevenzione dell'acquisizione di account (ATP)	Puoi rilevare e bloccare i tentativi di acquisizione di account con il nuovo gruppo di regole gestito per la prevenzione dell'acquisizione di account (ATP) di AWS WAF Fraud Control. `AWSManagedRulesATPRuleSet`	11 febbraio 2022
Regole gestite aggiornate AWS per AWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento dei seguenti gruppi di regole: Input non validi noti.	28 gennaio 2022
AWS WAF modifiche alle politiche gestite	Autorizzazioni `AWSWAFConsoleFullAccess` di registrazione aggiornate `AWSWAFFullAccessPolicy` e corrette.	11 gennaio 2022
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per AWS WAF aggiornare i seguenti gruppi di regole: core rule set (CRS), database SQLi.	10 gennaio 2022

Firewall Manager supporta la mitigazione automatica degli attacchi DDoS a livello di applicazione Shield Advanced	Le politiche Firewall Manager Shield Advanced per CloudFront le risorse Amazon ora includono il supporto per la mitigazione automatica degli attacchi DDoS a livello di applicazione.	7 gennaio 2022
AWS Firewall Manager modifica gestita delle politiche	Aggiorna a `FMSServiceRolePolicy` .	7 gennaio 2022
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento dei seguenti gruppi di regole: Input non validi noti.	17 dicembre 2021
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento dei seguenti gruppi di regole: Input non validi noti.	11 dicembre 2021
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento dei seguenti gruppi di regole: Input non validi noti.	10 dicembre 2021
Nuovo ruolo collegato al AWS Shield Advanced servizio	Aggiunto `AWSServiceRoleForAWSShield` per supportare la funzionalità di mitigazione degli attacchi DDoS a livello di applicazione automatica.	1° dicembre 2021

Nuova politica AWS Shield gestita	Aggiunto `AWSShield ServiceRolePolicy` per supportare la funzionalità di mitigazione degli attacchi DDoS a livello di applicazione automatica.	1° dicembre 2021
Opzione di mitigazione automatica degli attacchi DDoS a livello di applicazione ora disponibile con for AWS Shield Advanced CloudFront	Shield Advanced ora supporta la mitigazione automatica degli attacchi DDoS a livello di applicazione per le distribuzioni Amazon CloudFront. È possibile configurare Shield Advanced per contare o bloccare automaticamente le richieste Web che fanno parte di un attacco DDoS a livello di applicazione su una CloudFront distribuzione.	1° dicembre 2021
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento dei seguenti gruppi di regole: core rule set (CRS), sistema operativo Windows, sistema operativo Linux ed elenchi di reputazione IP.	23 novembre 2021
AWS Firewall Manager modifica gestita delle politiche	Aggiorna a`FMSServiceRolePolicy` .	18 novembre 2021

Opzioni di registrazione estese per AWS WAF	Ora puoi registrare il traffico ACL Web in un gruppo di log Amazon CloudWatch Logs o in un bucket Amazon Simple Storage Service (Amazon S3). Queste opzioni si aggiungon o all'opzione esistente di registrazione su Amazon Data Firehose.	15 novembre 2021
AWS WAF modifiche alle politiche gestite	Aggiornato `AWSWAFFul lAccessPolicy` e `AWSWAFConsoleFullA ccess` per supportare destinazioni di registrazione aggiuntive.	15 novembre 2021
AWS WAF nuova opzione di azione delle CAPTCHA regole	È possibile configurare le regole per eseguire un CAPTCHA in base alle richieste Web e, se necessari o, inviare un problema CAPTCHA al client.	8 novembre 2021
Regole gestite aggiornate per AWSAWS WAF	AWS Managed Rules per l' AWS WAF aggiornamento del gruppo di regole principali (CRS).	27 ottobre 2021
Regole AWS gestite aggiornat e per AWS WAF	Tutti i gruppi di regole AWS Managed Rules ora supportan o l'etichettatura. Le descrizio ni delle regole includono le specifiche dell'etichetta.	25 ottobre 2021

Firewall Manager supporta il filtraggio dei registri del Network Firewall	AWS Firewall Manager ora supporta il filtraggio dei log per le politiche di Network Firewall.	4 ottobre 2021
AWS Firewall Manager modifica gestita delle politiche	Aggiorna a`FMSServiceRolePolicy` .	29 settembre 2021
Aggiunta una dichiarazione di corrispondenza regex	Ora puoi abbinare le richieste web a una singola espressione regolare.	22 settembre 2021
Regole basate sulla tariffa all'interno AWS WAF dei gruppi di regole	È ora possibile definire regole basate sulle tariffe all'interno dei gruppi di regole. AWS WAF Nel AWS Firewall Manager, questa funzionalità è completamente supportata per le AWS WAF politiche.	13 settembre 2021
Firewall Manager supporta il filtraggio dei AWS WAF registri	AWS Firewall Manager ora supporta il filtraggio dei log per AWS WAF le policy.	31 agosto 2021
Rimuovi automaticamente le protezioni out-of-scope delle risorse in AWS Firewall Manager	AWS Firewall Manager consente di rimuovere automaticamente le protezioni dalle risorse che esulano dall'ambito delle politiche.	25 agosto 2021
AWS Firewall Manager modifica gestita delle politiche	Aggiorna a`FMSServiceRolePolicy` .	12 agosto 2021
È stato aggiunto il controllo delle versioni ai gruppi di regole gestiti	I fornitori di gruppi di regole gestiti possono ora modificare i propri gruppi di regole.	9 agosto 2021

Modifica i requisiti AWS Firewall Manager dell'amministratore	È possibile utilizzare l'account di gestione dell'organizzazione come account amministratore di Firewall Manager. Ciò non era consentito.	2 agosto 2021
Aumento della quota di Firewall Manager	È stato aumentato da 10 a 100 il numero di istanze Amazon VPC che puoi avere nell'ambito di una policy di Firewall Manager.	28 luglio 2021
AWS Firewall Manager supporto per il monitoraggio delle tabelle di AWS Network Firewall routing	AWS Firewall Manager ora supporta il monitoraggio della tabella delle rotte e fornisce consigli sulle azioni correttive e agli amministratori della sicurezza in caso di AWS Network Firewall politiche con percorsi configurati in modo errato.	8 luglio 2021
AWS WAF opzioni aggiuntive di trasformazione del testo	Opzioni estese per le trasformazioni del testo, che è possibile applicare ai componenti della richiesta Web prima di esaminarli.	24 giugno 2021
Denominazione modificata per le risorse relative alle AWS WAF policy di Firewall Manager	La denominazione degli ACL Web, dei gruppi di regole e della registrazione gestita da Firewall Manager per le AWS WAF policy è cambiata.	26 maggio 2021

Regole gestite aggiornate AWS per AWS WAF	AWS Regole gestite per AWS WAF aggiungere il supporto per l'etichettatura negli elenchi di reputazione IP e rimuovere i suffissi sui nomi delle regole per l'elenco di reputazione IP di Amazon.	4 maggio 2021
Aggiungi il supporto per Delegated Administrator AWS Organizations	Quando si imposta l'account AWS Firewall Manager amministratore, Firewall Manager ora designa l'account come amministratore AWS Organizations delegato per Firewall Manager. Con questa modifica, quando si imposta l'account amministr atore di Firewall Manager, è necessario fornire un account membro diverso dall'account di gestione dell'organizzazione. Questa modifica non influisce sulle impostazioni esistenti.	30 aprile 2021
Regole AWS gestite aggiornat e per AWS WAF	AWS Regole gestite per AWS WAF aver aggiunto il gruppo di regole AWS WAF Bot Control.	1 aprile 2021
Imposta le azioni delle regole individuali Count in un gruppo di regole	È ora possibile impostare le singole azioni delle regole in un gruppo di regole suCount. Le informazioni per l'override esistente, che si trova a livello di gruppo di regole, sono state corrette.	1 aprile 2021

Dichiarazione Scope-down per i gruppi di regole gestiti	È ora possibile utilizzare un'istruzione con ambito decrescente con i gruppi di regole gestiti nello stesso modo in cui è possibile utilizzare un'istruzione basata sulla frequenza.	1 aprile 2021
Filtraggio dei log	Ora puoi filtrare il traffico ACL Web registrato in base all'azione e all'etichetta delle regole.	1 aprile 2021
AWS WAF etichette sulle richieste web	È possibile configurare le regole per aggiungere etichette alle richieste Web corrispondenti e per applicarle alle etichette aggiunte da altre regole.	1 aprile 2021
AWS WAF Controllo dei bot	Puoi monitorare e controlla re il traffico dei bot con la nuova funzionalità AWS WAF Bot Control, che combina il gruppo di regole gestito da Bot Control con l'etichettatura delle richieste web, le istruzion i scope-down e il filtraggio dei log.	1 aprile 2021
Firewall Manager supporta le politiche del firewall DNS di Amazon Route 53 Resolver	AWS Firewall Manager supporta la gestione centraliz zata del filtraggio del traffico DNS in uscita di Amazon Route 53 Resolver DNS Firewall per i tuoi VPC.	31 marzo 2021

Gestione personalizzata di richieste e risposte	Puoi includere intestazioni personalizzate per le richieste Web che AWS WAF non bloccano e inviare risposte personalizzate per le richieste Web che AWS WAF bloccano. È disponibile per le impostazioni predefinite delle azioni Web ACL e delle azioni delle regole.	29 marzo 2021
AWS Firewall Manager modifica gestita delle politiche	Aggiorna a `FMSServiceRolePolicy` .	17 marzo 2021
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento dei seguenti gruppi di regole: core rule set (CRS), protezione degli amministratori, input noti non validi e sistema operativo Linux.	3 marzo 2021
AWS Shield monitoraggio gestito delle modifiche alle politiche	Shield ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	3 marzo 2021
AWS Firewall Manager monitoraggio gestito delle modifiche alle politiche	Firewall Manager ha iniziato a tenere traccia delle modifiche per le politiche AWS gestite.	2 marzo 2021
AWS WAF monitoraggio gestito delle modifiche alle politiche	AWS WAF ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	1 marzo 2021

Ispeziona il corpo di una richiesta web come JSON analizzato	È stata aggiunta l'opzione per ispezionare il corpo della richiesta Web come JSON analizzato e filtrato. Questa opzione si aggiunge all'opzione esistente per ispezionare il corpo della richiesta Web come testo semplice.	12 febbraio 2021
Firewall Manager supporta AWS Network Firewall le policy	AWS Firewall Manager supporta la gestione centrale del filtraggio del traffico di AWS Network Firewall rete per i tuoi VPC.	17 novembre 2020
Aggiungi il supporto per i gruppi di protezione AWS Shield Advanced	Ora puoi raggruppare le risorse protette in gruppi logici e gestirne le protezioni collettivamente.	13 Novembre 2020
È stato aggiunto il supporto per AWS AppSyncAWS WAF	Ora puoi associare un ACL AWS WAF web alla tua API AWS AppSync GraphQL. Questa modifica è disponibile solo nell'ultima versione di AWS WAF e non nella AWS WAF versione classica.	1 ottobre 2020
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento del set di regole del sistema operativo Windows.	23 settembre 2020
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per AWS WAF aggiornare i set di regole dell'applicazione PHP e del sistema operativo POSIX.	16 settembre 2020

Console aggiornata AWS Shield	AWS Shield offre una nuova opzione di console, con un'esperienza utente migliorata. Le indicazioni sulla console contenute nella documentazione si riferiscono alla nuova console.	1 settembre 2020
Firewall Manager si aggiorna alle politiche comuni dei gruppi di sicurezza	AWS Firewall Manager le politiche comuni dei gruppi di sicurezza ora supportano i tipi di risorse Application Load Balancers e Classic Load Balancers tramite l'implementazione della console. Le nuove opzioni sono disponibili nelle impostazioni dell'ambito delle politiche comuni.	11 agosto 2020
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento del set di regole di base.	7 agosto 2020
Firewall Manager supporta la AWS WAF configurazione della registrazione	AWS Firewall Manager ora supporta la configurazione di registrazione centralizzata per le politiche. AWS WAF	30 luglio 2020

Specificare la posizione dell'indirizzo IP nella richiesta web	È stata aggiunta l'opzione per utilizzare gli indirizzi IP da un'intestazione HTTP specificata dall'utente, anziché utilizzare l'origine della richiesta Web. L'intestazione alternativa è comunemente `X-Forwarded-For` (XFF), ma è possibile specificare qualsiasi nome di intestazione. È possibile utilizzare questa opzione per la corrispondenza dei set IP, la corrispondenza geografica e l'aggregazione del numero di regole basata sulla frequenza.	9 luglio 2020
Firewall Manager aggiorna le policy dei gruppi di sicurezza per il controllo dei contenuti	AWS Firewall Manager ha ampliato le funzionalità per le politiche di gruppo di sicurezza per il controllo dei contenuti, inclusa un'opzione di gestione delle regole, che utilizza elenchi di applicazioni e protocolli gestiti e dettagli sulle violazioni delle risorse.	7 luglio 2020
Elenchi gestiti da Firewall Manager	AWS Firewall Manager ora supporta elenchi gestiti di applicazioni e protocolli. Firewall Manager gestisce alcuni elenchi ed è possibile crearne e gestirne di propri.	7 luglio 2020

Firewall Manager supporta VPC condivisi nelle politiche comuni dei gruppi di sicurezza	AWS Firewall Manager ora supporta l'utilizzo di politiche di gruppo di sicurezza comuni in VPC condivisi. È possibile fare questo oltre a utilizzare tali policy nei VPC di proprietà degli account rientranti nell'ambito.	26 maggio 2020
Regole AWS gestite aggiornate per AWS WAF	Documentazione aggiunta per ogni regola in AWS Managed Rules for AWS WAF.	20 maggio 2020
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento del gruppo di regole del sistema operativo Linux.	19 maggio 2020
Aggiungi il supporto per la migrazione delle risorse AWS WAF Classic a AWS WAF (v2)	Ora puoi utilizzare la console o l'API per esportare le tue risorse AWS WAF Classic per la migrazione all'ultima versione di. AWS WAF	27 aprile 2020

Aggiungi il supporto per le unità AWS Organizations organizzative nell'ambito delle politiche	AWS Firewall Manager ora supporta l'utilizzo di unità AWS Organizations organizzative (OU) per specificare l'ambito delle politiche. È possibile utilizzare le unità organizza tive per includere o escludere account dall'ambito, oltre a includere o escludere account specifici. Specificare un'unità organizzativa equivale a specificare tutti gli account nell'unità organizzativa e in qualsiasi unità organizza tiva figlio, incluse le unità organizzative secondarie e gli account aggiunti in un secondo momento.	6 aprile 2020
Aggiungi il supporto per AWS WAF (v2) a AWS Firewall Manager	AWS Firewall Manager ora supporta la versione più recente AWS WAF, oltre alla versione precedente, di AWS WAF Classic.	31 marzo 2020
Aggiornamento alle politiche AWS Firewall Manager comuni dei gruppi di sicurezza	AWS Firewall Manager Common Security Group Policy ora ha la possibilità di applicare la policy a tutte le interfacce di rete elastiche nelle istanze Amazon EC2 pertinenti. È comunque possibile scegliere di applicare la policy solo all'interfaccia di rete elastica predefinita.	11 marzo 2020

Regole gestite aggiornate per AWSAWS WAF	AWS Regole gestite per AWS WAF aggiungere un gruppo di `AWSManagedRulesAnonymousIpList` regole.	6 marzo 2020
Regole AWS gestite aggiornate per AWS WAF	AWS Regole gestite per l' AWS WAF aggiornamento dell' WordPress applicazione e dei gruppi di `AWSManagedRulesCommonRuleSet` regole.	3 marzo 2020
Aggiunto il controllo dello stato di Amazon Route 53 alle opzioni di AWS Shield Advanced protezione	Shield Advanced ora supporta l'uso delle associazioni di controllo dello stato di Amazon Route 53, per migliorare l'accuratezza del rilevamento e della mitigazione delle minacce.	14 febbraio 2020
Regole AWS gestite aggiornate per AWS WAF	AWS Managed Rules for AWS WAF ha aggiornato il gruppo di regole del database SQL per aggiungere il controllo dell'URI del messaggio.	23 gennaio 2020

Firewall Manager: nuova opzione per la politica di controllo dell'utilizzo dei gruppi di sicurezza	Firewall Manager offre una nuova opzione per le politiche di controllo dell'utilizzo dei gruppi di sicurezza. È ora possibile impostare un numero minimo di minuti in cui un gruppo di sicurezza deve rimanere inutilizzato prima di essere considerato non conforme. Per impostazione predefinita, questa impostazi one dei minuti è zero.	14 gennaio 2020
Firewall Manager: nuova opzione per le AWS WAF policy	Firewall Manager offre una nuova opzione per AWS WAF le policy. È ora possibile scegliere di rimuovere tutte le associazioni di ACL Web esistenti dalle risorse nell'ambi to prima di associarle ai nuovi ACL Web della policy.	14 gennaio 2020
Regole AWS gestite aggiornat e per AWS WAF	AWS Managed Rules for AWS WAF ha aggiornato le trasformazioni di testo per le regole nel Core Rule Set e nei gruppi di regole del database SQL.	20 dicembre 2019
AWS Firewall Manager integrato con AWS Security Hub	AWS Firewall Manager ora crea i risultati relativi alle risorse non conformi e agli attacchi e li invia a AWS Security Hub.	18 dicembre 2019

Rilascio della AWS WAF versione 2	Nuova versione della guida per AWS WAF sviluppatori. Puoi gestire un'ACL Web o un gruppo di regole in formato JSON. Le funzionalità espanse includono istruzioni regola logiche, nidificazione delle istruzioni regola e supporto CIDR completo per indirizzi IP e intervalli di indirizzi. Le regole non sono più AWS risorse, ma esistono solo nel contesto di un ACL Web o di un gruppo di regole. Per i clienti esistenti, la versione precedente del servizio è ora denominata AWS WAF Classic. Nelle API, negli SDK e nelle CLI, AWS WAF Classic mantiene i propri schemi di denominazione e a quest'ult ima versione di AWS WAF si fa riferimento con l'aggiunta di «V2" o «v2", a seconda del contesto. AWS WAF non può accedere alle risorse create in Classic. AWS AWS WAF Per utilizzare tali risorse in AWS WAF, è necessario migrarle.	25 novembre 2019
AWS Gruppi di regole gestite per AWS WAF	Aggiunti gruppi di regole AWS Managed Rules. Questi sono gratuiti per AWS WAF i clienti.	25 novembre 2019

AWS Firewall Manager supporto per i gruppi di sicurezza di Amazon Virtual Private Cloud	È stato aggiunto il supporto per i gruppi di sicurezza Amazon VPC a Firewall Manager.	10 ottobre 2019
AWS Firewall Manager supporto per AWS Shield Advanced	È stato aggiunto il supporto per Shield Advanced a Firewall Manager.	15 marzo 2019
Tutorial: Creazione di politiche gerarchiche	Aggiunto il tutorial sulla creazione di policy gerarchiche in AWS Firewall Manager.	11 febbraio 2019
Controllo a livello di regole nei gruppi di regole	Ora puoi escludere singole regole dai gruppi di Marketpla ce AWS regole, oltre che dai tuoi gruppi di regole.	12 dicembre 2018
AWS Shield Advanced supporto per AWS Global Accelerator acceleratori standard	Shield Advanced ora può proteggere gli acceleratori AWS Global Accelerator standard.	26 novembre 2018
AWS WAF supporto per Amazon API Gateway	AWS WAF ora protegge le API di Amazon API Gateway.	25 ottobre 2018
Procedura guidata introduttiva avanzata di Expanded AWS Shield	La nuova procedura guidata offre l'opportunità di creare regole basate sulla tariffa e Amazon Events. CloudWatch	31 agosto 2018
AWS WAF logging	È possibile attivare la registraz ione per ottenere informazioni dettagliate sul traffico analizzat o dall'ACL Web.	31 agosto 2018

Support per i parametri di interrogazione in condizioni	Quando si crea una condizione, è ora possibile cercare le richieste per parametri specifici.	5 giugno 2018
Procedura guidata introduttiva avanzata di Shield	Introduce una nuova procedura semplificata per l'iscrizione a Shield AWS Advanced.	5 giugno 2018
Intervalli CIDR consentiti ampliati	Quando si crea una condizione di corrispondenza IP, AWS WAF ora supporta gli intervalli di indirizzi IPv4: /8 e qualsiasi intervallo compreso tra /16 e /32.	5 giugno 2018

Aggiornamenti prima del 2018

La tabella seguente descrive le modifiche importanti apportate in ogni versione della AWS WAF Developer Guide apportate prima del 2018.

Modifica	Versione API	Descrizione	Data di rilascio
Aggiornamento	24-08-2016	Marketplace AWS gruppi di regole	Novembre 2017
Aggiornamento	24-08-2016	Supporto Shield Advanced per indirizzi IP elastici	Novembre 2017
Aggiornamento	24-08-2016	Pannello di controllo globale delle minacce	Novembre 2017
Aggiornamento	24-08-2016	Tutorial di siti Web resistenti agli attacchi DDoS	Ottobre 2017

Modifica	Versione API	Descrizione	Data di rilascio
Aggiornamento	24-08-2016	Condizioni geografiche e regex	Ottobre 2017
Aggiornamento	24-08-2016	Regole basata sulla frequenza	Giugno 2017
Aggiornamento	24-08-2016	Riorganizzazione	Aprile 2017
Aggiornamento	24-08-2016	Aggiunte informazioni relative alla protezione DDOS e al supporto per sistemi di bilanciamento del carico delle applicazioni.	Novembre 2016
Nuove caratteristiche	24-08-2015	Ora puoi registrare tutte le tue chiamate API su AWS WAF Through AWS CloudTrail, il AWS servizio che registra le chiamate API per il tuo account e invia i file di registro al tuo bucket S3. CloudTrail i log possono essere utilizzati per consentire l'analisi della sicurezza , tenere traccia delle modifiche alle AWS risorse e facilitare il controllo della conformità. L'integrazione AWS WAF CloudTrail consente di determinare quali richieste sono state fatte all' AWS WAF API, l'indirizzo IP di origine da cui è stata effettuata ogni richiesta, chi ha effettuato la richiesta, quando è stata effettuata e altro ancora. Se lo stai già utilizzando AWS CloudTrail, inizierai a vedere le chiamate AWS WAF API nel tuo CloudTrail registro. Se non l'hai abilitato CloudTrail per il tuo account, puoi attivarlo CloudTrail da AWS Management Console. Non sono previsti costi aggiuntivi per l'attivazione CloudTrail, ma si applicano le tariffe standard per l'utilizzo di Amazon S3 e Amazon SNS.	28 aprile 2016

Modifica	Versione API	Descrizione	Data di rilascio
Nuove caratteristiche	24-08-2015	Ora puoi utilizzarlo AWS WAF per consentire, bloccare o contare le richieste Web che sembrano contenere script dannosi, il cosiddetto cross-site scripting o XSS. A volte gli aggressori inseriscono script dannosi nelle richieste Web nel tentativo di sfruttare le vulnerabilità delle applicazioni Web. Per ulteriori informazioni, consulta Istruzione regola di attacco di Cross-site scripting.	29 marzo 2016
Nuove caratteristiche	24-08-2015	Con questa versione, AWS WAF aggiunge le seguenti funzionalità: • È possibile configurare AWS WAF per consentire, bloccare o contare le richieste Web in base alla lunghezza di parti specifiche delle richieste, ad esempio stringhe di query o URI. Per ulteriori informazioni, consulta Istruzione regola vincolo di dimensioni. • È possibile configurare AWS WAF per consentire, bloccare o contare le richieste Web in base al contenuto nel corpo della richiesta. Questa è la parte di una richiesta che contiene i dati aggiuntivi da inviare al server Web come corpo della richiesta HTTP, come i dati provenienti da un modulo. Questa caratteristica si applica alle condizioni di corrispondenza stringa, alle condizioni di corrispondenza SQL injection e alle nuove condizioni per i vincoli di dimensioni menzionati nel primo elenco puntato. Per ulteriori informazioni, consulta Componenti delle richieste Web.	27 gennaio 2016

Modifica	Versione API	Descrizione	Data di rilascio
Nuova caratteristica	24-08-2015	È ora possibile utilizzare la AWS WAF console per scegliere le CloudFront distribuzioni a cui associare un ACL Web. Per ulteriori informazioni, consulta Associare o dissociare un ACL Web e una distribuzione. CloudFront	16 Novembre 2015
Versione iniziale	24-08-2015	Questa è la prima versione della Guida per sviluppatori di AWS WAF .	6 Ottobre 2015

AWS Glossario

Per la AWS terminologia più recente, consultate il AWS glossario nella sezione Reference.Glossario AWS

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.