



Entwicklerhandbuch

AWS WAF, AWS Firewall Manager, und AWS Shield Advanced



AWS WAFAWS Firewall Manager, und AWS Shield Advanced: Entwicklerhandbuch

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

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was sind AWS WAFAWS Shield und AWS Firewall Manager?	1
AWS WAF	1
AWS Shield	3
AWS Firewall Manager	4
Einrichtung	5
Melde dich an für eine AWS-Konto	5
Erstellen eines Administratorbenutzers	6
Tools herunterladen	7
AWS WAF	8
Wie AWS WAF funktioniert	9
AWS WAF Web-ACL-Kapazitätseinheiten (WCUs)	11
Ressourcen, mit denen Sie sich schützen können AWS WAF	13
Erste Schritte mit AWS WAF	14
Schritt 1: Einrichten AWS WAF	15
Schritt 2: Erstellen einer Web-ACL	15
Schritt 3: Hinzufügen einer Zeichenfolgen-Übereinstimmungsregel	17
Schritt 4: Fügen Sie eine Regelgruppe für AWS verwaltete Regeln hinzu	19
Schritt 5: Abschließen Ihrer Web-ACL-Konfiguration	20
Schritt 6: Bereinigen Ihrer Ressourcen	21
Web-Zugriffskontrolllisten (Web-ACLs)	22
Wie AWS Ressourcen mit Reaktionsverzögerungen umgehen von AWS WAF	23
Auswertung von Web-ACL-Regeln und -Regelgruppen	24
Die Web-ACL-Standardaktion	31
Verwaltung der Größenbeschränkungen bei Körperinspektionen	32
Konfiguration von CAPTCHA-, Challenge- und Token-Domänen	33
Arbeiten mit Web-ACLs	34
Regelgruppen	51
Verwaltete Regelgruppen	53
Verwaltung Ihrer eigenen Regelgruppen	226
Regelgruppen von anderen Services	232
Regeln	233
Regelaktion	235
Grundlagen der Regelerklärung	237
Regelaussagen abgleichen	263

Logische Regelaussagen	287
Ratenbasierte Regelanweisung	296
Regelanweisungen für Regelgruppen	316
Übergroße Komponenten für Webanfragen	319
Reguläre Ausdrücke	323
IP-Sets und Regex-Mustersätze	323
Erstellen und verwalten eines IP-Sets	324
Erstellen und Verwalten eines Regex-Mustersatzes	327
Benutzerdefinierte Webanforderungen und Antworten	330
Benutzerdefinierte Anforderungs-Header-Einfügungen	332
Benutzerdefinierte Antworten	334
Unterstützte Statuscodes	337
Bezeichnungen bei Webanforderungen	339
Funktionsweise von Bezeichnungen	341
Syntax- und Benennungsanforderungen	343
Hinzufügen einer Bezeichnung	346
Abgleich mit einer Bezeichnung	347
Beispiele für Bezeichnungsabgleich	349
Intelligente Abwehr von Bedrohungen	353
Optionen zur Risikominderung	354
Bewährte Methoden	368
Token für Webanfragen	371
Betrugsprävention bei der Kontoeröffnung	385
Verhinderung der Kontoübernahme	410
Bot-Steuerung	432
Integration von Client-Anwendungen	463
CAPTCHA und Challenge	501
AWS WAF Web-ACL-Verkehr protokollieren	514
Preise für die Protokollierung	515
AWS WAF Ziele protokollieren	516
Verwalten der Protokollierung für eine Web-ACL	529
Protokollfelder	531
Beispiele protokollieren	539
Testen und Optimieren Ihrer Schutzmaßnahmen	556
Testen und Optimieren von Schritten auf hoher Ebene	557
Vorbereitung für den Test	558

Überwachung und Tuning	561
Aktivierung Ihrer Schutzmaßnahmen in der Produktion	576
Wie AWS WAF funktioniert mit CloudFront Amazon-Funktionen	578
Verwendung AWS WAF mit CloudFront benutzerdefinierten Fehlerseiten	579
Verwenden Sie AWS WAF with CloudFront für Anwendungen, die auf Ihrem eigenen HTTP-Server ausgeführt werden	580
Auswahl der HTTP-Methoden, die CloudFront darauf reagieren	581
Sicherheit bei Ihrer Nutzung des AWS WAF Dienstes	581
Datenschutz	583
Identity and Access Management	584
Protokollierung und Überwachung	637
Compliance-Validierung	638
Ausfallsicherheit	640
Sicherheit der Infrastruktur	640
AWS WAF Kontingente	641
Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF	644
Warum migrieren zu AWS WAF?	645
So funktioniert die Migration	647
Migrationsvorbehalte	647
Migrieren einer Web-ACL	649
AWS WAF Klassisch	656
AWS WAF Classic einrichten	657
Melde dich an für ein AWS-Konto	5
Erstellen eines Administratorbenutzers	6
Tools herunterladen	659
So funktioniert AWS WAF Classic	660
AWS WAF Klassische Preisgestaltung	665
.....	665
Erste Schritte mit AWS WAF Classic	665
Schritt 1: Classic einrichten AWS WAF	667
Schritt 2: Erstellen einer Web-ACL	667
Schritt 3: Erstellen einer IP-Übereinstimmungsbedingung	668
Schritt 4: Erstellen einer Geo-Übereinstimmungsbedingung	669
Schritt 5: Erstellen einer Zeichenfolgen-Übereinstimmungsbedingung	670
Schritt 5A: Erstellen einer Regex-Bedingung (optional)	672
Schritt 6: Erstellen einer SQL Injection-Übereinstimmungsbedingung	674

Schritt 7: (Optional) Erstellen von zusätzlichen Bedingungen	676
Schritt 8: Erstellen einer Regel und Hinzufügen von Bedingungen	676
Schritt 9: Hinzufügen der Regel zu einer Web-ACL	679
Schritt 10: Bereinigen Ihrer Ressourcen	679
Erstellen und Konfigurieren einer Web-Zugriffskontrollliste (Web-ACL)	683
Verwenden von Bedingungen	685
Arbeiten mit Regeln	735
Arbeiten mit Web-ACLs	748
Arbeiten mit AWS WAF klassischen Regelgruppen zur Verwendung mit AWS Firewall Manager	764
Eine AWS WAF klassische Regelgruppe erstellen	765
Hinzufügen und Löschen von Regeln aus einer AWS WAF klassischen Regelgruppe	767
Erste Schritte mit AWS Firewall Manager , um AWS WAF klassische Regeln zu aktivieren	768
Schritt 1: Erfüllen der Voraussetzungen	769
Schritt 2: Erstellen von Regeln	770
Schritt 3: Erstellen einer Regelgruppe	770
Schritt 4: Eine AWS Firewall Manager AWS WAF Classic-Richtlinie erstellen und anwenden	772
Tutorial: Erstellen einer AWS Firewall Manager-Richtlinie mit hierarchischen Regeln	774
Schritt 1: Bestimmen Sie ein Firewall Manager Manager-Administratorkonto	775
Schritt 2: Erstellen Sie eine Regelgruppe mit dem Firewall Manager Manager- Administratorkonto	776
Schritt 3: Erstellen Sie eine Firewall Manager Manager-Richtlinie und fügen Sie die allgemeine Regelgruppe hinzu	776
Schritt 4: Hinzufügen kontospezifischer Regeln	777
Schlussfolgerung	777
Protokollieren von Web-ACL-Traffic-Informationen	777
Auflisten der durch ratenbasierte Regeln blockierten IP-Adressen	785
So funktioniert AWS WAF Classic mit CloudFront Amazon-Funktionen	786
Verwenden von AWS WAF Classic mit CloudFront benutzerdefinierten Fehlerseiten	787
Verwenden Sie AWS WAF Classic mit CloudFront für Anwendungen, die auf Ihrem eigenen HTTP-Server ausgeführt werden	787
Auswahl der HTTP-Methoden, die CloudFront darauf reagieren	788
Sicherheit	789
Datenschutz	790
Identity and Access Management	792

Protokollierung und Überwachung	820
Compliance-Validierung	821
Ausfallsicherheit	823
Sicherheit der Infrastruktur	823
AWS WAF Klassische Kontingente	824
AWS Shield	829
So funktionieren Shield und Shield Advanced	830
AWS Shield Standard Überblick	832
AWS Shield Advanced Überblick	832
Beispiele für DDoS-Angriffe	840
So erkennt Shield Ereignisse	841
Wie Shield Ereignisse abmildert	846
Beispiele für DDoS-resistente Architekturen	854
Beispiel für DDoS-Resilienz für Webanwendungen	855
Beispiel für DDoS-Resilienz für TCP- und UDP-Anwendungen	857
Beispiele für Shield Advanced-Anwendungsfälle	860
Erste Schritte	861
Abonnieren Sie Shield Advanced	862
Fügen Sie Ressourcen hinzu, um Schutzmaßnahmen zu schützen und zu konfigurieren	864
Konfigurieren Sie die SRT-Unterstützung	870
Erstellen Sie ein DDoS-Dashboard CloudWatch und stellen Sie Alarme ein CloudWatch	872
SRT-Unterstützung	873
Konfiguration des Zugriffs für das Shield Response Team (SRT)	874
Konfiguration von proaktivem Engagement	877
Kontaktaufnahme mit dem SRT	879
Konfiguration benutzerdefinierter Abhilfemaßnahmen mit dem SRT	880
Schutz von Ressourcen	881
Schutzmaßnahmen nach Ressourcentyp	881
Schutzmaßnahmen auf Anwendungsebene (Schicht 7)	883
Gesundheitsbasierte Erkennung mithilfe von Gesundheitschecks	903
Verwaltung des Ressourcenschutzes	916
Schutzgruppen	922
Verfolgen von Änderungen am Schutz	925
Einblick in DDoS-Ereignisse	926
Globale Aktivitäten und Kontoaktivitäten	927
Ereignisse	931

Kontoübergreifende Sichtbarkeit von Ereignissen	941
Reaktion auf DDoS-Ereignisse	943
Kontaktaufnahme mit dem Support wegen eines Angriffs auf Anwendungsebene	944
Manuelles Abwehren eines Angriffs auf Anwendungsebene	946
Nach einem Angriff eine Gutschrift beantragen	947
Sicherheit bei Ihrer Nutzung des Shield-Dienstes	949
Datenschutz	950
Identity and Access Management	951
Protokollierung und Überwachung	983
Compliance-Validierung	984
Ausfallsicherheit	985
Sicherheit der Infrastruktur	985
AWS Shield Advanced Kontingente	986
AWS Firewall Manager	987
AWS Firewall Manager Preisgestaltung	988
.....	988
AWS Firewall Manager Voraussetzungen	988
Schritt 1: Beitreten und konfigurieren AWS Organizations	989
Schritt 2: Erstellen Sie ein AWS Firewall Manager Standard-Administratorkonto	989
Schritt 3: Aktivieren AWS Config	991
Schritt 4: Abonnieren Sie Richtlinien für Drittanbieter im AWS Marketplace und konfigurieren Sie die Drittanbieter-Einstellungen	992
Schritt 5: Aktivieren Sie für Network Firewall- und DNS-Firewall-Richtlinien die gemeinsame Nutzung von Ressourcen	993
Schritt 6: Zur Verwendung AWS Firewall Manager in Regionen, die standardmäßig deaktiviert sind	994
Zusammenarbeit mit Firewall Manager Manager-Administratoren	994
Firewall Manager Manager-Administratorkonten erstellen, aktualisieren und sperren	996
Das Standard-Administratorkonto ändern	1000
Disqualifizierung von Änderungen an einem Administratorkonto	1001
Erste Schritte mit AWS Firewall Manager Richtlinien	1002
Erste Schritte mit AWS WAF Richtlinien	1003
Erste Schritte mit AWS Shield Advanced Richtlinien	1006
Erste Schritte mit Amazon VPC-Sicherheitsgruppenrichtlinien	1011
Erste Schritte mit AWS Network Firewall Richtlinien	1015
Erste Schritte mit DNS-Firewall-Richtlinien	1019

Erste Schritte mit den Palo Alto Networks Cloud NGFW-Richtlinien	1021
Erste Schritte mit den Fortigate CNF-Richtlinien	1025
Mit AWS Firewall Manager Richtlinien arbeiten	1029
Allgemeine Einstellungen	1030
Erstellen einer Richtlinie	1030
Löschen einer Richtlinie	1070
Geltungsbereich der Politik	1071
Verwaltete Listen	1073
AWS WAF Richtlinien	1079
AWS Shield Advanced Richtlinien	1090
Richtlinien für Sicherheitsgruppen	1096
Netzwerk-Firewall-Richtlinien	1110
DNS-Firewall-Richtlinien	1122
Die NGFW-Richtlinien von Palo Alto Networks Cloud	1124
Fortigate CNF-Richtlinien	1124
Gemeinsame Nutzung von Ressourcen für Network Firewall- und DNS-Firewall- Richtlinien	1125
Mit Ressourcensätzen arbeiten	1127
Überlegungen bei der Arbeit mit Ressourcensätzen in Firewall Manager	1127
Ressourcensets erstellen	1128
.....	1129
Konformität für eine Richtlinie anzeigen	1130
Ergebnisse von Firewall Manager	1135
AWS WAF politische Feststellungen	1136
Ergebnisse der Shield-Politik	1137
Allgemeine Richtlinienerkenntnisse der Sicherheitsgruppe	1137
Erkenntnisse der Prüfungsrichtlinie für Sicherheitsgruppen	1138
Erkenntnisse der Überwachungsrichtlinie für Sicherheitsgruppen	1138
Ergebnisse der DNS-Firewall-Richtlinie	1139
Sicherheit	1140
Datenschutz	1141
Identitäts- und Zugriffsverwaltung	1142
Protokollierung und Überwachung	1185
Compliance-Validierung	1186
Ausfallsicherheit	1187
Sicherheit der Infrastruktur	1187

AWS Firewall Manager Kontingente	1188
Weiche Kontingente	1188
Feste Kontingente	1191
Überwachen	1193
Überwachungstools	1194
Automatisierte Überwachungstools	1194
Manuelle Tools	1196
Überwachung mit CloudWatch	1196
Anzeigen von -Metriken und -Dimensionen	1197
AWS WAF Metriken und Dimensionen	1198
AWS Shield Advanced Metriken	1208
AWS Firewall Manager Benachrichtigungen	1214
Protokollierung von AWS CloudTrail-API-Aufrufen mit	1214
AWS WAF Informationen in AWS CloudTrail	1215
AWS Shield Advanced Informationen in CloudTrail	1225
AWS Firewall Manager Informationen in CloudTrail	1227
Verwenden der AWS WAF AWS Shield Advanced and-API	1230
Verwendung der AWS SDKs	1230
HTTPS-Anfragen an AWS WAF oder Shield Advanced stellen	1230
Anforderungs-URI	1230
HTTP-Header	1231
HTTP-Anforderungstext	1232
HTTP-Antworten	1233
Fehlermeldungen	1234
Authentifizieren von Anforderungen	1234
Ähnliche Informationen	1237
Dokumentverlauf	1239
Updates vor 2018	1291
AWS Glossar	1295
.....	mccxcvi

Was sind AWS WAF, AWS Shield und AWS Firewall Manager?

Sie können [AWS WAF](#), und [AWS Firewall Manager](#) zusammen verwenden [AWS Shield](#), um eine umfassende Sicherheitslösung zu erstellen. AWS WAF ist eine Firewall für Webanwendungen, mit der Sie Webanfragen überwachen können, die Ihre Endbenutzer an Ihre Anwendungen senden, und den Zugriff auf Ihre Inhalte kontrollieren können. AWS Shield bietet Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) auf AWS Ressourcen, auf der Netzwerk- und Transportebene (Schicht 3 und 4) und auf der Anwendungsebene (Schicht 7). AWS Firewall Manager ermöglicht die Verwaltung von Schutzmaßnahmen wie AWS WAF, AWS Shield Advanced für Konten und Ressourcen, auch wenn neue Ressourcen hinzugefügt werden.

Themen

- [AWS WAF](#)
- [AWS Shield](#)
- [AWS Firewall Manager](#)

AWS WAF

AWS WAF ist eine Firewall für Webanwendungen, mit der Sie die HTTP- und HTTPS-Anfragen überwachen können, die an Ihre geschützten Webanwendungsressourcen weitergeleitet werden. Sie können die folgenden Ressourcentypen schützen:

- CloudFront Amazon-Vertrieb
- Amazon API Gateway API-Gateway-REST-API
- Application Load Balancer
- AWS AppSync GraphQL-API
- Amazon-Cognito-Benutzerpool
- AWS App Runner Dienst
- AWS Instanz mit verifiziertem Zugriff

AWS WAF ermöglicht es Ihnen, den Zugriff auf Ihre Inhalte zu kontrollieren. Basierend auf von Ihnen angegebenen Bedingungen, z. B. den IP-Adressen, von denen Anfragen stammen, oder den Werten

von Abfragezeichenfolgen, beantwortet Ihre geschützte Ressource Anfragen entweder mit dem angeforderten Inhalt, mit einem HTTP-Statuscode 403 (Forbidden) oder mit einer benutzerdefinierten Antwort.

Auf der einfachsten Ebene AWS WAF können Sie eines der folgenden Verhaltensweisen wählen:

- Alle Anfragen außer den von Ihnen angegebenen zulassen — Dies ist nützlich, wenn Sie möchten, dass Amazon CloudFront, Amazon API Gateway, Application Load Balancer AWS AppSync, Amazon Cognito oder AWS Verified Access Inhalte für eine öffentliche Website bereitstellen, aber auch Anfragen von Angreifern blockieren möchten. AWS App Runner
- Alle Anfragen außer den von Ihnen angegebenen blockieren — Dies ist nützlich, wenn Sie Inhalte für eine eingeschränkte Website bereitstellen möchten, deren Benutzer leicht anhand von Eigenschaften in Webanfragen identifiziert werden können, z. B. anhand der IP-Adressen, die sie zum Aufrufen der Website verwenden.
- Zählen Sie Anfragen, die Ihren Kriterien entsprechen — Sie können die Count Aktion verwenden, um Ihren Web-Traffic zu verfolgen, ohne die Art und Weise, wie Sie damit umgehen, zu ändern. Sie können dies für die allgemeine Überwachung und auch zum Testen Ihrer neuen Regeln für die Bearbeitung von Webanfragen verwenden. Wenn Sie Anfragen zulassen oder blockieren möchten, die auf neuen Eigenschaften in den Webanfragen basieren, können Sie zunächst konfigurieren AWS WAF , dass die Anfragen gezählt werden, die diesen Eigenschaften entsprechen. Auf diese Weise können Sie Ihre neuen Konfigurationseinstellungen bestätigen, bevor Sie Ihre Regeln ändern, um übereinstimmende Anfragen zuzulassen oder zu blockieren.
- Führen Sie CAPTCHA- oder Challenge-Checks für Anfragen durch, die Ihren Kriterien entsprechen — Sie können CAPTCHA- und Silent-Challenge-Kontrollen für Anfragen implementieren, um den Bot-Traffic zu Ihren geschützten Ressourcen zu reduzieren.

Die Verwendung AWS WAF hat mehrere Vorteile:

- Zusätzlicher Schutz vor Webangriffen anhand von Kriterien, die Sie angeben. Sie können Kriterien anhand von Merkmalen von Webanfragen wie den folgenden definieren:
 - IP-Adressen, von denen Anforderungen stammen.
 - Land, aus dem die Anfragen stammen.
 - Werte in Anforderungs-Headern.
 - Zeichenfolgen, die in Anfragen vorkommen, entweder bestimmte Zeichenfolgen oder Zeichenfolgen, die Mustern regulärer Ausdrücke (Regex) entsprechen.
 - Länge der Anforderungen.

- Vorhandensein von möglicherweise schädlichem SQL-Code (SQL Injections).
- Vorhandensein eines möglicherweise schädlichen Skripts (Cross-Site Scripting).
- Regeln, die Webanfragen, die die angegebenen Kriterien erfüllen, zulassen, blockieren oder zählen können. Alternativ können Regeln Webanfragen blockieren oder zählen, die nicht nur die angegebenen Kriterien erfüllen, sondern auch eine bestimmte Anzahl von Anfragen in einer Minute oder in fünf Minuten überschreiten.
- Regeln, die Sie für mehrere Webanwendungen verwenden können.
- Verwaltete Regelgruppen von AWS und AWS Marketplace Verkäufern.
- Echtzeitmetriken und Stichproben-Webanforderungen.
- Automatisierte Verwaltung mithilfe der AWS WAF API.

Wenn Sie eine detaillierte Kontrolle über die Schutzmaßnahmen haben möchten, die Sie Ihren Ressourcen hinzufügen, könnte dies AWS WAF allein die richtige Wahl sein. Weitere Informationen zu finden Sie AWS WAF unter. [AWS WAF](#)

AWS Shield

Sie können AWS WAF Web Access Control Lists (Web-ACLs) verwenden, um die Auswirkungen eines Distributed Denial of Service (DDoS) -Angriffs zu minimieren. Für zusätzlichen Schutz vor DDoS-Angriffen bietet auch AWS und. AWS Shield Standard AWS Shield Advanced AWS Shield Standard ist automatisch und ohne zusätzliche Kosten enthalten, die über das hinausgehen, wofür Sie bereits bezahlen, AWS WAF und für Ihre anderen AWS Dienste.

AWS Shield Advanced bietet erweiterten Schutz vor DDoS-Angriffen für Ihre Amazon EC2 EC2-Instances, Elastic Load Balancing Load Balancer, CloudFront Distributionen, Route 53-Hosting-Zonen und Standardbeschleuniger. AWS Global Accelerator AWS Shield Advanced fallen zusätzliche Gebühren an. Zu den Optionen und Funktionen von Shield Advanced gehören automatische DDoS-Abwehr auf Anwendungsebene, erweiterte Sichtbarkeit von Ereignissen und engagierter Support durch das Shield Response Team (SRT). Wenn Sie Websites mit hoher Sichtbarkeit besitzen oder anderweitig häufig DDoS-Angriffen ausgesetzt sind, sollten Sie den Kauf der zusätzlichen Schutzmaßnahmen, die Shield Advanced bietet, in Betracht ziehen. Weitere Informationen finden Sie unter [AWS Shield Advanced Fähigkeiten und Optionen](#) und [Entscheidung, ob zusätzliche Schutzmaßnahmen abonniert AWS Shield Advanced und angewendet werden sollen](#).

AWS Firewall Manager

AWS Firewall Manager vereinfacht Ihre Verwaltungs- und Wartungsaufgaben für mehrere Konten und Ressourcen und bietet eine Vielzahl von Schutzmaßnahmen AWS WAF, AWS Shield Advanced, darunter Amazon VPC-Sicherheitsgruppen und Amazon Route 53 Resolver DNS Firewall. AWS Network Firewall Mit Firewall Manager richten Sie Ihre Schutzmaßnahmen nur einmal ein und der Service wendet sie automatisch auf Ihre Konten und Ressourcen an, auch wenn Sie neue Konten und Ressourcen hinzufügen.

Weitere Informationen zu Firewall Manager finden Sie unter [AWS Firewall Manager](#).

Einrichtung

In diesem Thema werden vorläufige Schritte beschrieben, z. B. das Erstellen eines Kontos, um Sie auf die Verwendung von AWS WAF AWS Firewall Manager, und vorzubereiten AWS Shield Advanced. Diese vorläufigen Artikel werden Ihnen nicht in Rechnung gestellt. Ihnen werden nur die AWS Dienste in Rechnung gestellt, die Sie in Anspruch nehmen.

Themen

- [Melde dich an für eine AWS-Konto](#)
- [Erstellen eines Administratorbenutzers](#)
- [Tools herunterladen](#)

Melde dich an für eine AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie <https://portal.aws.amazon.com/billing/signup>.
2. Folgen Sie den Online-Anweisungen.

Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Tasten eingeben.

Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontos wird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem [Administratorbenutzer Administratorzugriff](#) zu und verwenden Sie nur den Root-Benutzer, um [Aufgaben auszuführen, die Root-Benutzerzugriff](#) erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu <https://aws.amazon.com/> auf und klicken Sie auf Mein Konto.

Erstellen eines Administratorbenutzers

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich [AWS Management Console](#) als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter [Anmelden als Root-Benutzer](#) im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

Anweisungen finden Sie unter [Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer \(Konsole\)](#) im IAM-Benutzerhandbuch.

Erstellen eines Administratorbenutzers

1. Aktivieren Sie das IAM Identity Center.

Anweisungen finden Sie unter [Aktivieren AWS IAM Identity Center](#) im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Administratorzugriff.

Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter [Benutzerzugriff mit der Standardeinstellung konfigurieren](#).AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie [im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal](#).

Tools herunterladen

Das AWS Management Console beinhaltet eine Konsole für AWS WAF, und AWS Shield Advanced AWS Firewall Manager, aber wenn Sie programmgesteuert auf die Dienste zugreifen möchten, finden Sie folgende Informationen:

- Die API-Anleitungen dokumentieren die von den Services unterstützten Operationen und enthalten Links zur entsprechenden SDK- und CLI-Dokumentation:
 - [AWS WAF API Reference](#)
 - [AWS Shield Advanced API Reference](#)
 - [AWS Firewall Manager API Reference](#)
- Um eine API aufzurufen, ohne sich um Details auf niedriger Ebene wie das Zusammenstellen von HTTP-Anfragen kümmern zu müssen, können Sie ein AWS SDK verwenden. Die AWS SDKs stellen Funktionen und Datentypen bereit, die die Funktionalität von Diensten zusammenfassen. AWS Informationen zum Herunterladen eines AWS SDK und zum Zugriff auf Installationsanweisungen finden Sie auf der entsprechenden Seite:
 - [Java](#)
 - [JavaScript](#)
 - [.NET](#)
 - [Node.js](#)
 - [PHP](#)
 - [Python](#)
 - [Ruby](#)

Eine vollständige Liste der AWS SDKs finden Sie unter [Tools für Amazon Web Services](#).

- Sie können die AWS Command Line Interface (AWS CLI) verwenden, um mehrere AWS Dienste von der Befehlszeile aus zu steuern. Sie können Ihre Befehle auch mithilfe von Skripts automatisieren. Weitere Informationen finden Sie unter [AWS Command Line Interface](#).
- AWS Tools for Windows PowerShell unterstützt diese AWS Dienste. Weitere Informationen finden Sie in der [AWS Tools for PowerShell -Cmdlet-Referenz](#).

AWS WAF

AWS WAF ist eine Firewall für Webanwendungen, mit der Sie die HTTP (S) -Anfragen überwachen können, die an Ihre geschützten Webanwendungsressourcen weitergeleitet werden. Sie können die folgenden Ressourcentypen schützen:

- CloudFront Amazon-Vertrieb
- Amazon API Gateway API-Gateway-REST-API
- Application Load Balancer
- AWS AppSync GraphQL-API
- Amazon-Cognito-Benutzerpool
- AWS App Runner Dienst
- AWS Instanz mit verifiziertem Zugriff

AWS WAF ermöglicht es Ihnen, den Zugriff auf Ihre Inhalte zu kontrollieren. Basierend auf von Ihnen angegebenen Kriterien, wie den IP-Adressen, von denen Anfragen stammen, oder den Werten von Abfragezeichenfolgen, beantwortet der mit Ihrer geschützten Ressource verknüpfte Dienst Anfragen entweder mit dem angeforderten Inhalt, mit einem HTTP-403-Statuscode (Forbidden) oder mit einer benutzerdefinierten Antwort.

Note

Sie können es auch AWS WAF zum Schutz Ihrer Anwendungen verwenden, die in Amazon Elastic Container Service (Amazon ECS) -Containern gehostet werden. Amazon ECS ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Docker-Containern in einem Cluster vereinfacht. Um diese Option zu verwenden, konfigurieren Sie Amazon ECS so, dass ein Application Load Balancer verwendet wird, der für die AWS WAF Weiterleitung und den Schutz von HTTP (S) -Layer-7-Verkehr zwischen den Aufgaben in Ihrem Service aktiviert ist. Weitere Informationen finden Sie unter [Service – Load Balancing](#) im Amazon-Elastic-Container-Service-Entwicklerhandbuch.

Themen

- [Wie AWS WAF funktioniert](#)

- [Erste Schritte mit AWS WAF](#)
- [Web-Zugriffskontrolllisten \(Web-ACLs\)](#)
- [Regelgruppen](#)
- [AWS WAF Regeln](#)
- [Umgang mit übergroßen Webanforderungskomponenten in AWS WAF](#)
- [Musterabgleich mit regulären Ausdrücken in AWS WAF](#)
- [IP-Sätze und Regex-Mustersätze in AWS WAF](#)
- [Benutzerdefinierte Webanforderungen und Antworten in AWS WAF](#)
- [AWS WAF Labels auf Webanfragen](#)
- [AWS WAF intelligente Bedrohungsabwehr](#)
- [AWS WAF Web-ACL-Verkehr protokollieren](#)
- [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#)
- [Wie AWS WAF funktioniert mit CloudFront Amazon-Funktionen](#)
- [Sicherheit bei der Nutzung des AWS WAF Dienstes](#)
- [AWS WAF Kontingente](#)
- [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#)

Wie AWS WAF funktioniert

Sie steuern AWS WAF damit, wie Ihre geschützten Ressourcen auf HTTP (S) -Webanfragen reagieren. Dazu definieren Sie eine Web Access Control List (ACL) und ordnen sie dann einer oder mehreren Webanwendungsressourcen zu, die Sie schützen möchten. Die zugehörigen Ressourcen leiten eingehende Anfragen AWS WAF zur Prüfung durch die Web-ACL weiter.

In Ihrer Web-ACL erstellen Sie Regeln, um Verkehrsmuster zu definieren, nach denen in Anfragen gesucht werden soll, und um festzulegen, welche Aktionen bei entsprechenden Anfragen ergriffen werden sollen. Zu den Aktionsoptionen gehören die folgenden:

- Erlauben Sie, dass die Anfragen zur Verarbeitung und Beantwortung an die geschützte Ressource weitergeleitet werden.
- Blockieren Sie die Anfragen.
- Zählen Sie die Anfragen.

- Führen Sie CAPTCHA- oder Challenge-Checks anhand von Anfragen durch, um zu überprüfen, ob menschliche Benutzer und Standardbrowser verwendet werden.

AWS WAF Komponenten

Die folgenden sind die zentralen Komponenten von AWS WAF:

- Web-ACLs — Sie verwenden eine Web-Zugriffskontrollliste (ACL), um eine Reihe von AWS Ressourcen zu schützen. Sie erstellen eine Web-ACL und definieren deren Schutzstrategie, indem Sie Regeln hinzufügen. Regeln definieren Kriterien für die Prüfung von Webanfragen und legen fest, welche Maßnahmen bei Anfragen ergriffen werden sollen, die ihren Kriterien entsprechen. Sie legen außerdem eine Standardaktion für die Web-ACL fest, die angibt, ob Anfragen blockiert oder zugelassen werden sollen, die die Regeln noch nicht blockiert oder zugelassen haben. Weitere Informationen zu Web-ACLs finden Sie unter [Web-Zugriffskontrolllisten \(Web-ACLs\)](#).

Eine Web-ACL ist eine AWS WAF Ressource.

- Regeln – Jede Regel enthält eine Anweisung, die die Überprüfungskriterien definiert, und eine Maßnahme, die zu ergreifen ist, wenn eine Webanforderung die Kriterien erfüllt. Wenn eine Webanfrage die Kriterien erfüllt, ist das eine Übereinstimmung. Sie können Regeln konfigurieren, um passende Anfragen zu blockieren, sie durchzulassen, sie zu zählen oder Botkontrollen gegen sie auszuführen, die CAPTCHA-Rätsel oder stille Client-Browser-Challenges verwenden. Weitere Informationen zu Regeln finden Sie unter [AWS WAF Regeln](#).

Eine Regel ist keine Ressource. AWS WAF Sie ist nur im Kontext einer Web-ACL oder Regelgruppe vorhanden.

- Regelgruppen — Sie können Regeln direkt in einer Web-ACL oder in wiederverwendbaren Regelgruppen definieren. AWS Verwaltete Regeln und AWS Marketplace Verkäufer stellen verwaltete Regelgruppen für Sie bereit. Sie können auch eigene Regelgruppen definieren. Weitere Informationen zu Regelgruppen finden Sie unter [Regelgruppen](#).

Eine Regelgruppe ist eine AWS WAF Ressource.

Themen

- [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#)
- [Ressourcen, mit denen Sie sich schützen können AWS WAF](#)

AWS WAF Web-ACL-Kapazitätseinheiten (WCUs)

AWS WAF verwendet Web-ACL-Kapazitätseinheiten (WCU), um die Betriebsressourcen zu berechnen und zu steuern, die für die Ausführung Ihrer Regeln, Regelgruppen und Web-ACLs erforderlich sind. AWS WAF setzt WCU-Grenzwerte durch, wenn Sie Ihre Regelgruppen und Web-ACLs konfigurieren. WCUs haben keinen Einfluss darauf, wie AWS WAF der Web-Traffic untersucht wird.

AWS WAF verwaltet die Kapazität für Regeln, Regelgruppen und Web-ACLs.

Regel-WCUs

AWS WAF berechnet die Regelkapazität, wenn Sie eine Regel erstellen oder aktualisieren. AWS WAF berechnet die Kapazität für jeden Regeltyp unterschiedlich, um die relativen Kosten jeder Regel widerzuspiegeln. Einfache Regeln, die bei der Ausführung wenig Aufwand erfordern, verwenden weniger WCUs als komplexere Regeln, die mehr Rechenleistung verbrauchen. Beispielsweise verwendet eine Regel zur Größenbeschränkung weniger WCUs als eine Anweisung, die Anfragen anhand eines Regex-Mustersatzes untersucht.

Die Kapazitätsanforderungen für Regeln beginnen im Allgemeinen bei den Grundkosten für den Regeltyp und nehmen mit der Komplexität zu, z. B. wenn Sie vor der Prüfung Texttransformationen hinzufügen oder wenn Sie den JSON-Text überprüfen. Informationen zu den Kapazitätsanforderungen für Regeln finden Sie in den Auflistungen der Regelanweisungen unter [Grundlagen der Regelerklärung](#).

Regelgruppe WCUs

Die WCU-Anforderungen für eine Regelgruppe werden durch die Regeln bestimmt, die Sie innerhalb der Regelgruppe definieren. Die maximale Kapazität für eine Regelgruppe beträgt 5.000 WCUs.

Jede Regelgruppe hat eine unveränderliche Kapazitätseinstellung, die der Besitzer bei der Erstellung zuweist. Dies gilt für verwaltete Regelgruppen und Regelgruppen, mit denen Sie sie erstellen. AWS WAF Wenn Sie eine Regelgruppe ändern, müssen Ihre Änderungen dafür sorgen, dass die WCUs der Regelgruppe im Rahmen ihrer Kapazität bleiben. Dadurch wird sichergestellt, dass Web-ACLs, die die Regelgruppe verwenden, ihren Kapazitätsanforderungen entsprechen.

Die in einer Regelgruppe verwendeten WCUs sind die Summe der WCUs für die Regeln abzüglich aller Verarbeitungsoptimierungen, die durch die AWS WAF Kombination des Verhaltens der Regeln erzielt werden können. Wenn Sie beispielsweise zwei Regeln definieren, um dieselbe Webanforderungskomponente zu untersuchen, und die Regeln jeweils eine bestimmte

Transformation auf die Komponente anwenden, bevor sie überprüft wird, AWS WAF kann Ihnen möglicherweise nur einmal für die Anwendung der Transformation eine Gebühr berechnet werden. Die WCU-Kosten für die Verwendung einer Regelgruppe in einer Web-ACL entsprechen immer der festen WCU-Einstellung, die Sie bei der Erstellung der Regelgruppe definiert haben.

Achten Sie beim Erstellen einer Regelgruppe darauf, dass die Kapazität hoch genug ist, um die Regeln zu berücksichtigen, die Sie während der gesamten Lebensdauer der Regelgruppe verwenden möchten.

Web-ACL-WCUs

Die WCU-Anforderungen für eine Web-ACL werden durch die Regeln und Regelgruppen bestimmt, die Sie in der Web-ACL verwenden.

- Die Kosten für die Verwendung einer Regelgruppe in einer Web-ACL hängen von der Kapazitätseinstellung der Regelgruppe ab.
- Die Kosten für die Verwendung einer Regel sind die berechneten WCUs der Regel abzüglich aller Verarbeitungsoptimierungen, die AWS WAF aus der Regelkombination der Web-ACL erzielt werden können. Wenn Sie beispielsweise zwei Regeln definieren, um dieselbe Webanforderungskomponente zu untersuchen, und die Regeln jeweils eine bestimmte Transformation auf die Komponente anwenden, bevor sie überprüft wird, AWS WAF kann Ihnen möglicherweise nur einmal für die Anwendung der Transformation eine Gebühr berechnet werden.

Der Grundpreis für eine Web-ACL beinhaltet bis zu 1.500 WCUs. Für die Nutzung von mehr als 1.500 WCUs fallen gemäß einem gestaffelten Preismodell zusätzliche Gebühren an. AWS WAF passt Ihre Web-ACL-Preise automatisch an, wenn sich Ihre Web-ACL-WCU-Nutzung ändert. Details zu den Preisen finden Sie unter [AWS WAF -Preise](#).

Die maximale Kapazität für eine Web-ACL beträgt 5.000 WCUs.

Bestimmung der WCU-Nutzung

Wie in den vorherigen Abschnitten erwähnt, entspricht die Gesamtzahl der in einer Regelgruppe oder Web-ACL verwendeten WCUs der Summe der WCUs für alle Regeln, die in der Regelgruppe oder Web-ACL definiert sind, oder darunter.

In der AWS WAF Konsole können Sie sehen, wie viel Kapazität verbraucht wird, wenn Sie Ihrer Web-ACL oder Regelgruppe Regeln hinzufügen. In der Konsole werden die aktuell verwendeten Kapazitätseinheiten angezeigt, wenn Sie die Regeln hinzufügen.

Über die API können Sie die maximalen Kapazitätsanforderungen für die Regeln überprüfen, die Sie in einer Web-ACL oder Regelgruppe verwenden möchten. Geben Sie dazu die JSON-Liste der Regeln für den Check Capacity-Aufruf an. Weitere Informationen finden Sie [CheckCapacity](#) in der AWS WAF V2-API-Referenz.

Ressourcen, mit denen Sie sich schützen können AWS WAF

Sie können eine AWS WAF Web-ACL verwenden, um globale oder regionale Ressourcentypen zu schützen. Dazu ordnen Sie die Web-ACL den Ressourcen zu, die Sie schützen möchten. Die Web-ACL und alle von ihr verwendeten AWS WAF Ressourcen müssen sich in der Region befinden, in der sich die zugehörige Ressource befindet. Für CloudFront Amazon-Distributionen ist dies auf USA Ost (Nord-Virginia) festgelegt.

CloudFront Amazon-Distributionen

Mithilfe der AWS WAF Konsole oder der APIs können Sie einer CloudFront Distribution eine AWS WAF Web-ACL zuordnen. Sie können einer CloudFront Distribution auch eine Web-ACL zuordnen, wenn Sie die Distribution selbst erstellen oder aktualisieren. Um eine Zuordnung zu konfigurieren AWS CloudFormation, müssen Sie die CloudFront Verteilungskonfiguration verwenden. Informationen zu Amazon CloudFront finden Sie im Amazon CloudFront Developer Guide unter [Using AWS WAF to Control Access to Your Content](#).

AWS WAF ist weltweit für den CloudFront Vertrieb verfügbar, aber Sie müssen die Region USA Ost (Nord-Virginia) verwenden, um Ihre Web-ACL und alle in der Web-ACL verwendeten Ressourcen wie Regelgruppen, IP-Sets und Regex-Mustersätze zu erstellen. Einige Benutzeroberflächen bieten die Regionsauswahl „Global ()CloudFront“. Diese Auswahl ist identisch mit der Auswahl der Region USA Ost (Nord-Virginia) oder "us-east-1".

Regionale Ressourcen

Sie können regionale Ressourcen in allen Regionen schützen, in denen sie AWS WAF verfügbar sind. Sie finden die Liste unter [AWS WAF Endpunkte und Kontingente](#) im Allgemeine Amazon Web Services-Referenz.

Sie können AWS WAF zum Schutz der folgenden regionalen Ressourcentypen verwenden:

- Amazon API Gateway API-Gateway-REST-API
- Application Load Balancer
- AWS AppSync GraphQL-API
- Amazon-Cognito-Benutzerpool

- AWS App Runner Dienst
- AWS Instanz mit verifiziertem Zugriff

Sie können eine Web-ACL nur einem darin enthaltenen Application Load Balancer zuordnen. AWS-Regionen Sie können beispielsweise einem aktiven Application Load Balancer keine Web-ACL zuordnen. AWS Outposts

Die Web-ACL und alle anderen AWS WAF Ressourcen, die sie verwendet, müssen sich in derselben Region wie die geschützten Ressourcen befinden. Bei der Überwachung und Verwaltung von Webanfragen für eine geschützte regionale Ressource werden alle Daten in derselben Region AWS WAF aufbewahrt wie die geschützte Ressource.

Einschränkungen für mehrere Ressourcenzuordnungen

Sie können eine einzelne Web-ACL mit einer oder mehreren AWS Ressourcen verknüpfen, wobei die folgenden Einschränkungen gelten:

- Sie können jede AWS Ressource nur einer Web-ACL zuordnen. Die Beziehung zwischen Web-ACL und AWS Ressourcen ist one-to-many.
- Sie können eine Web-ACL einer oder mehreren CloudFront Distributionen zuordnen. Sie können eine Web-ACL, die Sie einer CloudFront Distribution zugeordnet haben, keinem anderen AWS Ressourcentyp zuordnen.

Erste Schritte mit AWS WAF

Dieses Tutorial zeigt, wie Sie AWS WAF die folgenden Aufgaben ausführen können:

- Einrichten AWS WAF.
- Erstellen Sie mit dem Assistenten in der AWS WAF Konsole eine Web-Zugriffskontrollliste (Web-ACL).
- Wählen Sie die AWS Ressourcen aus, für AWS WAF die Sie Webanfragen überprüfen möchten. Dieses Tutorial behandelt die Schritte für Amazon CloudFront. Der Prozess ist im Wesentlichen derselbe für eine Amazon API Gateway Gateway-REST-API, einen Application Load Balancer, eine AWS AppSync GraphQL-API, einen Amazon Cognito Cognito-Benutzerpool, einen AWS App Runner Service oder eine AWS Verified Access-Instance.
- Fügen Sie die Regeln und Regelgruppen hinzu, die Sie zum Filtern von Webanforderungen verwenden möchten. Sie können beispielsweise die IP-Adressen angeben, von denen die

Anfragen stammen, und Werte in der Anfrage angeben, die nur von Angreifern verwendet werden. Sie geben für jede Regel an, wie übereinstimmende Webanforderungen behandelt werden. Sie können sie beispielsweise blockieren oder zählen und Bot-Herausforderungen wie CAPTCHA ausführen. Sie definieren für jede Regel, die Sie in einer Web-ACL definieren, und für jede Regel, die Sie in einer Regelgruppe definieren, eine Aktion.

- Geben Sie eine Standardaktion für die Web-ACL an (entweder Block oder Allow). Dies ist die Aktion, die AWS WAF bei einer Anfrage ausgeführt wird, wenn die Regeln in der Web-ACL sie nicht ausdrücklich zulassen oder blockieren.

Note

AWS In der Regel werden Ihnen für die Ressourcen, die Sie in diesem Tutorial erstellen, weniger als 0,25 USD pro Tag in Rechnung gestellt. Wenn Sie das Tutorial beendet haben, empfehlen wir, dass Sie die Ressourcen löschen, um unnötige Kosten zu vermeiden.

Themen

- [Schritt 1: Einrichten AWS WAF](#)
- [Schritt 2: Erstellen einer Web-ACL](#)
- [Schritt 3: Hinzufügen einer Zeichenfolgen-Übereinstimmungsregel](#)
- [Schritt 4: Fügen Sie eine Regelgruppe für AWS verwaltete Regeln hinzu](#)
- [Schritt 5: Abschließen Ihrer Web-ACL-Konfiguration](#)
- [Schritt 6: Bereinigen Ihrer Ressourcen](#)

Schritt 1: Einrichten AWS WAF

Wenn Sie die allgemeinen Einrichtungsschritte unter noch nicht befolgt haben [Einrichtung](#), tun Sie dies jetzt.


Schritt 2: Erstellen einer Web-ACL

Die AWS WAF Konsole führt Sie Schritt für Schritt durch den Konfigurationsprozess, AWS WAF um Webanfragen auf der Grundlage von von Ihnen festgelegter Kriterien zu blockieren oder zuzulassen, wie z. B. die IP-Adressen, von denen die Anfragen stammen, oder die Werte in den Anfragen. In

diesem Schritt erstellen Sie eine Web-ACL. Weitere Informationen zu AWS WAF Web-ACLs finden Sie unter [Web-Zugriffskontrolllisten \(Web-ACLs\)](#).


So erstellen Sie eine Web-ACL

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie auf der AWS WAF Startseite die Option Web-ACL erstellen aus.
3. Geben Sie unter Name den Namen ein, mit dem Sie diese Web-ACL bezeichnen möchten.

 Note

Sie können den Namen nach dem Erstellen der Web-ACL nicht mehr ändern.

4. (Optional) Geben Sie für Description - optional (Beschreibung–optional) eine längere Beschreibung für die Web-ACL ein, wenn Sie möchten.
5. Ändern Sie für den CloudWatch Metrikenamen gegebenenfalls den Standardnamen. Befolgen Sie die Anweisungen zu gültigen Zeichen in der Konsole. Der Name darf keine Sonderzeichen, Leerzeichen oder für AWS WAF reservierte Metrikenamen enthalten, einschließlich "All" und "Default_Action".

 Note

Sie können den CloudWatch Metrikenamen nicht mehr ändern, nachdem Sie die Web-ACL erstellt haben.

6. Wählen Sie als Ressourcentyp die Option CloudFrontDistributionen aus. Die Region wird bei Verteilungen automatisch mit Global (CloudFront) aufgefüllt. CloudFront
7. (Optional) Wählen Sie unter Zugeordnete AWS Ressourcen — optional die Option Ressourcen hinzufügen AWS aus. Wählen Sie im Dialogfeld die Ressourcen aus, die Sie verknüpfen möchten, und klicken Sie dann auf Hinzufügen. AWS WAF kehrt zur Seite „Web-ACL und zugehörige AWS Ressourcen beschreiben“ zurück.
8. Wählen Sie Weiter aus.

Schritt 3: Hinzufügen einer Zeichenfolgen-Übereinstimmungsregel

In diesem Schritt erstellen Sie eine Regel mit einer Zeichenfolgen-Übereinstimmungsanweisung und geben an, was mit übereinstimmenden Anforderungen zu tun ist. Eine Zeichenfolgen-Übereinstimmungsregelanweisung identifiziert Zeichenfolgen, nach denen Sie AWS WAF in einer Anforderung suchen lassen möchten. Eine Zeichenfolge besteht aus druckbaren ASCII-Zeichen, aber Sie können beliebige Zeichen aus dem hexadezimalen Bereich von 0x00 bis 0xFF (dezimal 0 bis 255) angeben. Zusätzlich zur Angabe der Zeichenfolge, nach der gesucht werden soll, geben Sie die zu suchende Webanforderungskomponente an, etwa einen Header, eine Abfragezeichenfolge oder den Anforderungstext.

Dieser Anweisungstyp arbeitet mit einer Webanforderungskomponente und erfordert die folgenden Einstellungen für Anforderungskomponenten:

- Anforderungskomponente — Der Teil der Webanforderung, der überprüft werden soll, z. B. eine Abfragezeichenfolge oder der Hauptteil.

Warning

Wenn Sie die Anforderungskomponenten Body, JSON-Text, Header oder Cookies untersuchen, sollten Sie sich über die Einschränkungen informieren, mit denen der Inhalt überprüft AWS WAF werden kann. [Umgang mit übergroßen Webanforderungskomponenten in AWS WAF](#)

Informationen über Webanforderungskomponenten finden Sie unter [Webanforderungskomponenten](#).

- Optionale Texttransformationen — Transformationen, die Sie an der Anforderungskomponente durchführen AWS WAF möchten, bevor Sie sie überprüfen. Sie könnten beispielsweise in Kleinschreibung umwandeln oder Leerzeichen normalisieren. Wenn Sie mehr als eine Transformation angeben, werden diese in der angegebenen Reihenfolge AWS WAF verarbeitet. Weitere Informationen finden Sie unter [Texttransformationen](#).

Weitere Informationen zu AWS WAF Regeln finden Sie unter [AWS WAF Regeln](#).

So erstellen Sie eine Anweisung zur Erstellung einer Zeichenfolgen-Übereinstimmungsregel

1. Wählen Sie auf der Seite Add rules and rule groups (Regeln und Regelgruppen hinzufügen) Add rules (Regeln hinzufügen), Add my own rules and rule groups (Eigene Regeln und Regelgruppen hinzufügen), Rule-Builder und Rule visual editor (Visueller Regel-Editor).

Note

Die Konsole stellt den Visuellen Regel-Editor und einen JSON-Regel-Editor zur Verfügung. Der JSON-Editor erleichtert das Kopieren von Konfigurationen zwischen Web-ACLs und ist für komplexere Regelsätze erforderlich, wie beispielsweise solche mit mehreren Verschachtelungsebenen.

Bei diesem Verfahren wird der Visuelle Regel-Editor verwendet.

2. Geben Sie unter Name den Namen ein, mit dem Sie diese Regel bezeichnen möchten.
3. Wählen Sie für Type (Typ) Rule (Regel).
4. Für If a request (Wenn eine Anforderung) wählen Sie matches the statement (entspricht der Anweisung) aus.

Die anderen Optionen sind für die logischen Regelanweisungstypen bestimmt. Diese können sie verwenden, um die Ergebnisse anderer Regelanweisungen zu kombinieren oder zu negieren.

5. Öffnen Sie unter Statement für Inspect die Dropdownliste und wählen Sie die Webanforderungskomponente aus, die Sie überprüfen AWS WAF möchten. Wählen Sie für dieses Beispiel Header aus.

Wenn Sie Header wählen, geben Sie auch an, welchen Header AWS WAF prüfen soll. Geben Sie **User-Agent** ein. Dieser Wert wird nicht nach Groß- und Kleinschreibung unterschieden.

6. Wählen Sie für Match type (Übereinstimmungstyp) aus, wo die angegebene Zeichenfolge im User-Agent-Header erscheinen soll.

Wählen Sie für dieses Beispiel Exactly matches string (Stimmt exakt mit Zeichenfolge überein). Dies bedeutet, dass der User-Agent-Header in jeder Webanforderung auf eine Zeichenfolge AWS WAF überprüft wird, die mit der von Ihnen angegebenen Zeichenfolge identisch ist.

7. Legen Sie für String to match (Zeichenfolge für Übereinstimmung) eine Zeichenkette fest, nach der AWS WAF suchen soll. Die maximale Länge von String to match (Zeichenfolge für Übereinstimmung) beträgt 200 Zeichen. Wenn Sie einen base64-codierten Wert angeben möchten, können Sie vor der Kodierung bis zu 200 Zeichen angeben.

Geben Sie für dieses Beispiel ein. MyAgent AWS WAF untersucht den User-Agent Header in Webanfragen auf den Wert MyAgent.

8. Lassen Sie Text transformation (Texttransformation) auf None (Keine).
9. Wählen Sie unter Action (Aktion) die Aktion aus, die die Regel ausführen soll, wenn sie einer Webanforderung entspricht. Wählen Sie in diesem Beispiel Count (Anzahl) und lassen Sie die anderen Optionen so, wie sie sind. Durch die Aktion „Count“ (Anzahl) werden Metriken für Webanforderungen erstellt, die mit der Regel übereinstimmen (ohne Einfluss darauf, ob die Anforderung zugelassen oder blockiert ist). Weitere Informationen zur Auswahl von Aktionen finden Sie unter [Regelaktion](#) und [Auswertung von Web-ACL-Regeln und -Regelgruppen](#).
10. Wählen Sie Regel hinzufügen aus.

Schritt 4: Fügen Sie eine Regelgruppe für AWS verwaltete Regeln hinzu

AWS Managed Rules bietet Ihnen eine Reihe von verwalteten Regelgruppen, von denen die meisten für AWS WAF Kunden kostenlos sind. Weitere Informationen zu Regelgruppen finden Sie unter [Regelgruppen](#). Wir fügen dieser Web-ACL eine Regelgruppe für AWS verwaltete Regeln hinzu.

Um eine Regelgruppe für AWS verwaltete Regeln hinzuzufügen

1. Wählen Sie auf der Seite Add rules and rule groups (Regeln und Regelgruppen hinzufügen) Add rules (Regeln hinzufügen), und wählen Sie dann Add managed rule groups (Verwaltete Regelgruppen hinzufügen).
2. Erweitern Sie auf der Seite Add managed rule groups (Verwaltete Regelgruppen hinzufügen) die Auflistung für die Verwalteten AWS -Regelgruppen. (Es werden auch Angebote für AWS Marketplace Verkäufer angezeigt. Sie können ihre Angebote abonnieren und sie dann genauso verwenden wie für Regelgruppen mit AWS verwalteten Regeln.)
3. Führen Sie die folgenden Schritte für die Regelgruppe aus, die Sie hinzufügen möchten:
 - a. Aktivieren Sie die Option Add to web ACL (Zur Web-ACL hinzufügen) in der Spalte Action (Aktion).
 - b. Wählen Sie Bearbeiten aus und öffnen Sie in der Liste Regeln der Regelgruppe die Dropdownliste Alle Regelaktionen außer Kraft setzen und wählen Sie aus Count. Dadurch wird festgelegt, dass alle Regeln in der Regelgruppe nur zählen. Auf diese Weise können Sie sehen, wie sich alle Regeln der Regelgruppe mit Ihren Webanforderungen verhalten, bevor Sie einzelne davon verwenden.

- c. Wählen Sie Save rule (Regel speichern).
4. Wählen Sie auf der Seite Add managed rule groups (Verwaltete Regelgruppen hinzufügen) die Option Add rules (Regeln hinzufügen). Nun werden Sie wieder zur Seite Add rules and rule groups (Regeln und Regelgruppen hinzufügen) geleitet.

Schritt 5: Abschließen Ihrer Web-ACL-Konfiguration

Wenn Sie mit dem Hinzufügen von Regeln und Regelgruppen zu Ihrer Web-ACL-Konfiguration fertig sind, verwalten Sie abschließend die Priorität der Regeln in der Web-ACL und konfigurieren Einstellungen wie Metriken, Tagging und Protokollierung.

So schließen Sie Ihre Web-ACL-Konfiguration ab

1. Wählen Sie auf der Seite Add rules and rule groups (Regeln und Regelgruppen hinzufügen) die Option Next (Weiter).
2. Auf der Seite Regelpriorität festlegen können Sie die Verarbeitungsreihenfolge für die Regeln und Regelgruppen in der Web-ACL sehen. AWS WAF verarbeitet sie ab dem Anfang der Liste. Sie können die Verarbeitungsreihenfolge ändern, indem Sie die Regeln nach oben oder unten verschieben. Wählen Sie dazu eine in der Liste aus und wählen Sie Move up (Nach oben verschieben) oder Move down (Nach unten verschieben). Weitere Informationen zur Priorität von Regeln finden Sie unter [Reihenfolge der Verarbeitung von Regeln und Regelgruppen in einer Web-ACL](#).
3. Wählen Sie Weiter aus.
4. Auf der Seite Metriken konfigurieren für CloudWatch Amazon-Metriken können Sie die geplanten Metriken für Ihre Regeln und Regelgruppen sowie die Sampling-Optionen für Webanfragen einsehen. Informationen zum Anzeigen von Stichprobenanforderungen finden Sie unter [Anzeigen einer Stichprobe von Webanforderungen](#). Informationen zu CloudWatch Amazon-Metriken finden Sie unter [Überwachung mit Amazon CloudWatch](#).

Sie können auf der Seite der Web-ACL in der AWS WAF Konsole unter dem Tab Traffic-Übersicht auf Zusammenfassungen der Metriken zum Web-Traffic zugreifen. Die Konsolen-Dashboards bieten fast in Echtzeit Zusammenfassungen der CloudWatch Amazon-Metriken der Web-ACL. Weitere Informationen finden Sie unter [Dashboards zur Übersicht über den Web-ACL-Verkehr](#).

5. Wählen Sie Weiter.

- Überprüfen Sie auf der Seite Review and create web ACL (Überprüfen und Web-ACL erstellen) Ihre Einstellungen und wählen Sie dann Create web ACL (Web-ACL erstellen).

Der Assistent kehrt zur Seite Web ACL zurück, auf der Ihre neue Web-ACL aufgelistet ist.

Schritt 6: Bereinigen Ihrer Ressourcen

Sie haben das Tutorial jetzt erfolgreich abgeschlossen. Um zu verhindern, dass für Ihr Konto zusätzliche AWS WAF Gebühren anfallen, sollten Sie die von Ihnen erstellten AWS WAF Objekte bereinigen. Alternativ können Sie die Konfiguration so ändern, dass sie den Webanfragen entspricht, die Sie tatsächlich verwalten möchten. AWS WAF

Note

AWS berechnet Ihnen in der Regel weniger als 0,25 USD pro Tag für die Ressourcen, die Sie in diesem Tutorial erstellen. Wenn Sie fertig sind, empfehlen wir, dass Sie die Ressourcen löschen, um unnötige Kosten zu vermeiden.

Um die Objekte zu löschen, für die AWS WAF Gebühren anfallen

- Wählen Sie auf der Seite Web ACL Ihre Web-ACL aus der Liste aus und wählen Sie Edit (Bearbeiten).
- Wählen Sie auf der Registerkarte Zugeordnete AWS Ressourcen für jede zugeordnete Ressource das Optionsfeld neben dem Ressourcennamen aus, und klicken Sie dann auf Zuordnung trennen. Dadurch wird die Web-ACL von Ihren AWS Ressourcen getrennt.
- Wählen Sie auf der der folgenden Seiten Next (Weiter), bis Sie zur Seite Web ACL zurückkehren.

Wählen Sie auf der Seite Web ACL Ihre Web-ACL aus der Liste aus und wählen Sie Delete (Löschen).

Regeln und Regelnweisungen existieren nicht außerhalb der Definitionen von Regelgruppen und Web-ACLs. Wenn Sie eine Web-ACL löschen, werden alle einzelnen Regeln gelöscht, die Sie in der Web-ACL definiert haben. Wenn Sie eine Regelgruppe aus einer Web-ACL entfernen, entfernen Sie einfach den Verweis darauf.

Web-Zugriffskontrolllisten (Web-ACLs)

Eine Web-Zugriffssteuerungsliste (Web-ACL) ermöglicht eine differenzierte Kontrolle aller HTTP(S)-Webanforderungen, auf die Ihre geschützte Ressource reagiert. Sie können Ressourcen von Amazon CloudFront, Amazon API Gateway, Application Load Balancer AWS AppSync, Amazon Cognito und AWS Verified Access schützen. AWS App Runner

Sie können Kriterien wie die folgenden verwenden, um Anforderungen zuzulassen oder zu blockieren:

- Ursprung der IP-Adresse der Anforderung
- Ursprungsland der Anforderung
- Zeichenfolgen-Übereinstimmung oder Regex-Übereinstimmung in einem Teil der Anforderung
- Größe eines bestimmten Teils der Anforderung
- Erkennen von schädlichem SQL-Code oder Skripting

Sie können die Anforderungen auch auf jede beliebige Kombination dieser Bedingungen überprüfen. Sie können Webanfragen blockieren oder zählen, die nicht nur die angegebenen Bedingungen erfüllen, sondern auch eine bestimmte Anzahl von Anfragen in einer Minute überschreiten. Sie können Bedingungen über logische Operatoren kombinieren. Sie können auch CAPTCHA-Rätsel und unbeaufsichtigte Client-Sitzungen anhand von Anfragen ausführen.

In den AWS WAF Regelanweisungen geben Sie Ihre Übereinstimmungskriterien und die Maßnahmen an, die Sie bei Übereinstimmungen ergreifen sollen. Sie können Regelanweisungen direkt in Ihrer Web-ACL und in wiederverwendbaren Regelgruppen definieren, die Sie in Ihrer Web-ACL verwenden. Eine vollständige Liste der Optionen finden Sie unter [Grundlagen der Regelerklärung](#) und [Regelaktion](#).

Um Ihre Prüf- und Behandlungskriterien für Webanforderungen festzulegen, führen Sie die folgenden Aufgaben aus:

1. Wählen Sie die Web-ACL-Standardaktion (entweder Allow oder Block) für Webanfragen, die keiner der von Ihnen angegebenen Regeln entsprechen. Weitere Informationen finden Sie unter [Die Web-ACL-Standardaktion](#).
2. Fügen Sie alle Regelgruppen hinzu, die Sie in Ihrer Web-ACL verwenden möchten. Verwaltete Regelgruppen enthalten normalerweise Regeln, die Webanfragen blockieren. Informationen zu Regelgruppen finden Sie unter [Regelgruppen](#).

3. Geben Sie in einer oder mehreren Regeln zusätzliche Übereinstimmungskriterien und Handlungsanweisungen an. Um mehr als eine Regel hinzuzufügen, beginnen Sie mit AND- oder OR-Regelanweisungen und verschachteln Sie die Regeln, die Sie unter diesen kombinieren möchten. Wenn Sie eine Regeloption negieren möchten, verschachteln Sie die Regel in einer NOT-Anweisung. Sie können optional eine ratenbasierte Regel anstelle einer regulären Regel verwenden, um die Anzahl der Anforderungen einer einzelnen IP-Adresse, die die Bedingungen erfüllt, zu begrenzen. Informationen zu Regeln finden Sie unter [AWS WAF Regeln](#).

Wenn Sie einer Web-ACL mehr als eine Regel hinzufügen, werden die Regeln in der Reihenfolge AWS WAF ausgewertet, in der sie für die Web-ACL aufgeführt sind. Weitere Informationen finden Sie unter [Auswertung von Web-ACL-Regeln und -Regelgruppen](#).

Wenn Sie eine Web-ACL erstellen, geben Sie die Arten von Ressourcen an, mit denen Sie sie verwenden möchten. Weitere Informationen finden Sie unter [Erstellen einer Web-ACL](#). Nachdem Sie eine Web-ACL definiert haben, können Sie sie mit Ihren Ressourcen verknüpfen, um mit dem Schutz für sie zu beginnen. Weitere Informationen finden Sie unter [Zuordnen oder Aufheben der Zuordnung einer Web-ACL zu einer Ressource AWS](#).

Wie AWS Ressourcen mit Reaktionsverzögerungen umgehen von AWS WAF

In einigen Fällen AWS WAF kann ein interner Fehler auftreten, der die Antwort auf die Frage, AWS ob eine Anfrage zugelassen oder blockiert werden soll, verzögert. In diesen Fällen CloudFront wird die Anfrage in der Regel zugelassen oder der Inhalt bereitgestellt, während die Regionaldienste die Anfrage in der Regel ablehnen und den Inhalt nicht bereitstellen.

Themen

- [Auswertung von Web-ACL-Regeln und -Regelgruppen](#)
- [Die Web-ACL-Standardaktion](#)
- [Verwaltung der Größenbeschränkungen bei Körperinspektionen](#)
- [CAPTCHA-, Challenge- und Token-Domain-Konfiguration für eine Web-ACL](#)
- [Arbeiten mit Web-ACLs](#)

Auswertung von Web-ACL-Regeln und -Regelgruppen

Die Art und Weise, wie eine Web-ACL eine Webanforderung behandelt, hängt von folgenden Faktoren ab:

- Die numerischen Prioritätseinstellungen der Regeln in der Web-ACL und in Regelgruppen
- Die Aktionseinstellungen für die Regeln und die Web-ACL
- Alle Überschreibungen, die Sie an den Regeln in den Regelgruppen vornehmen, die Sie hinzufügen

Eine Liste der Einstellungen für Regelaktionen finden Sie unter [Regelaktion](#).

Sie können die Anforderungs- und Antwortbehandlung in den Einstellungen für Regelaktionen und in den Einstellungen für standardmäßige Web-ACL-Aktionen anpassen. Weitere Informationen finden Sie unter [Benutzerdefinierte Webanforderungen und Antworten in AWS WAF](#).

Themen

- [Reihenfolge der Verarbeitung von Regeln und Regelgruppen in einer Web-ACL](#)
- [So werden Regel- und Regelgruppenaktionen in einer Web-ACL behandelt](#)
- [Aktionsüberschreibungen in Regelgruppen](#)

Reihenfolge der Verarbeitung von Regeln und Regelgruppen in einer Web-ACL

In einer Web-ACL und in einer Regelgruppe bestimmen mithilfe von numerischen Prioritätseinstellungen, in welcher Reihenfolge die Regeln ausgewertet werden. Sie müssen für jede Regel in einer Web-ACL eine eindeutige Prioritätseinstellung innerhalb dieser Web-ACL festlegen und für jede Regel in einer Regelgruppe eine eindeutige Prioritätseinstellung innerhalb dieser Regelgruppe festlegen.

Note

Wenn Sie Regelgruppen und AWS WAF Web-ACLs über die Konsole verwalten, weist Ihnen anhand der Reihenfolge der Regeln in der Liste eindeutige numerische Prioritätseinstellungen zu. AWS WAF weist der Regel oben in der Liste die niedrigste numerische Priorität und der Regel unten die höchste numerische Priorität zu.

Bei der AWS WAF Auswertung einer Web-ACL oder Regelgruppe anhand einer Webanforderung werden die Regeln von der Einstellung mit der niedrigsten numerischen Priorität bis entweder eine Übereinstimmung gefunden, die die Auswertung beendet, oder bis alle Regeln aufgebraucht sind.

Angenommen, Ihre Web-ACL enthält die folgenden Regeln und Regelgruppen mit diesen Prioritäten:

- Regel1 – Priorität 0
- RuleGroupA — Priorität 100
 - RegelA1 – Priorität 10.000
 - RegelA2 – Priorität 20.000
- Regel2 – Priorität 200
- RuleGroupB — Priorität 300
 - RegelB1 – Priorität 0
 - RegelB2 – Priorität 1

AWS WAF würde die Regeln für diese Web-ACL in der folgenden Reihenfolge auswerten:

- Regel 1
- RuleGroupEine Regel A1
- RuleGroupEine Regel A2
- Regel 2
- RuleGroupVon RuleB1
- RuleGroupVon RuleB2

So werden Regel- und Regelgruppenaktionen in einer Web-ACL behandelt

Wenn Sie Ihre Regeln und Regelgruppen konfigurieren, wählen Sie aus, wie Sie passende Webanfragen behandeln AWS WAF möchten:

- Allow und Block beenden Aktionen — Allow und Block Aktionen beenden jegliche andere Verarbeitung der Web-ACL für die entsprechende Webanforderung. Wenn eine Regel in einer Web-ACL eine Entsprechung für eine Anfrage findet und die Regelaktion Allow oder lautet Block, bestimmt diese Übereinstimmung die endgültige Disposition der Webanforderung für die Web-ACL. AWS WAF verarbeitet keine anderen Regeln in der Web-ACL, die auf die entsprechende Regel folgen. Dies gilt für Regeln, die Sie direkt zur Web-ACL hinzufügen, und Regeln, die sich innerhalb

einer hinzugefügten Regelgruppe befinden. Mit der Block Aktion empfängt oder verarbeitet die geschützte Ressource die Webanforderung nicht.

- **Count** ist eine Aktion, die nicht beendet wird — Wenn eine Regel mit einer Count Aktion einer Anfrage entspricht, AWS WAF zählt die Anfrage und setzt dann die Verarbeitung der Regeln fort, die im Web-ACL-Regelsatz folgen.
- **CAPTCHA** und **es Challenge** kann sich um Aktionen handeln, die nicht beenden oder beenden — Wenn eine Regel mit einer dieser Aktionen einer Anfrage entspricht, AWS WAF wird ihr Token-Status überprüft. Wenn die Anforderung über ein gültiges Token verfügt, AWS WAF behandelt sie ähnlich wie eine Count Übereinstimmung und setzt dann die Verarbeitung der Regeln fort, die im Web-ACL-Regelsatz folgen. Wenn die Anfrage kein gültiges Token hat, wird die Auswertung AWS WAF beendet und dem Client ein CAPTCHA-Rätsel oder eine Aufforderung zur Lösung einer Clientsitzung im Hintergrund gesendet.

Wenn die Regelauswertung zu keiner abschließenden Aktion führt, wird die Web-ACL-Standardaktion auf die Anfrage AWS WAF angewendet. Weitere Informationen finden Sie unter [Die Web-ACL-Standardaktion](#).

In Ihrer Web-ACL können Sie die Aktionseinstellungen für Regeln in einer Regelgruppe überschreiben. Außerdem haben Sie die Möglichkeit, die Aktion zu überschreiben, die von einer Regelgruppe zurückgegeben wird. Weitere Informationen finden Sie unter [Aktionsüberschreibungen in Regelgruppen](#).

Interaktion zwischen Aktionen und Prioritätseinstellungen

Die Aktionen, die AWS WAF für eine Webanforderung gelten, werden von den numerischen Prioritätseinstellungen der Regeln in der Web-ACL beeinflusst. Angenommen, Ihre Web-ACL hat eine Regel mit Allow Aktion und einer numerischen Priorität von 50 und eine weitere Regel mit Count Aktion und einer numerischen Priorität von 100. AWS WAF wertet die Regeln in einer Web-ACL in der Reihenfolge ihrer Priorität aus, beginnend mit der niedrigsten Einstellung, sodass die Zulassungsregel vor der Zählregel ausgewertet wird. Eine Webanforderung, die beiden Regeln entspricht, entspricht zuerst der Zulassungsregel. Da Allow es sich um eine abschließende Aktion handelt, AWS WAF wird die Auswertung bei dieser Übereinstimmung gestoppt und die Anfrage nicht anhand der Zählregel bewertet.

- Wenn Sie nur Anfragen, die nicht der Zulassungsregel entsprechen, in Ihre Kennzahlen zur Zählregel aufnehmen möchten, dann würden die Prioritätseinstellungen der Regeln funktionieren.

- Wenn Sie dagegen Metriken aus der Zählregel auch für Anfragen zählen möchten, die der Zulassungsregel entsprechen, müssten Sie der Zählregel eine niedrigere numerische Priorität zuweisen als der Zulassungsregel, sodass sie zuerst ausgeführt wird.

Weitere Informationen zu Prioritätseinstellungen finden Sie unter [Reihenfolge der Verarbeitung von Regeln und Regelgruppen in einer Web-ACL](#).

Aktionsüberschreibungen in Regelgruppen

Wenn Sie Ihrer Web-ACL eine Regelgruppe hinzufügen, können Sie die Aktionen überschreiben, die sie bei entsprechenden Webanfragen ausführt. Durch das Überschreiben der Aktionen für eine Regelgruppe in Ihrer Web-ACL-Konfiguration wird die Regelgruppe selbst nicht geändert. Es ändert nur, wie die Regelgruppe im Kontext der Web-ACL AWS WAF verwendet wird.

Regelaktionen überschreiben

Sie können die Aktionen der Regeln innerhalb einer Regelgruppe durch jede gültige Regelaktion überschreiben. Wenn Sie dies tun, werden übereinstimmende Anfragen genauso behandelt, als ob die Aktion der konfigurierten Regel die Einstellung zum Außerkraftsetzen wäre.

Note

Regelaktionen können beendend oder nicht beendend sein. Eine abschließende Aktion stoppt die Web-ACL-Auswertung der Anfrage und lässt sie entweder an Ihre geschützte Anwendung weiterleiten oder blockiert sie.

Hier sind die Optionen für die Regelaktion:

- **Allow**— AWS WAF ermöglicht die Weiterleitung der Anfrage zur Bearbeitung und Beantwortung an die geschützte AWS Ressource. Dies ist eine abschließende Aktion. In von Ihnen definierten Regeln können Sie benutzerdefinierte Header in die Anfrage einfügen, bevor Sie sie an die geschützte Ressource weiterleiten.
- **Block**— AWS WAF blockiert die Anfrage. Dies ist eine abschließende Aktion. Standardmäßig antwortet Ihre geschützte AWS Ressource mit einem 403 (Forbidden) HTTP-Statuscode. In Regeln, die Sie definieren, können Sie die Antwort anpassen. Wenn eine Anfrage AWS WAF blockiert wird, bestimmen die Block Aktionseinstellungen die Antwort, die die geschützte Ressource an den Client zurücksendet.

- **Count**— AWS WAF zählt die Anfrage, bestimmt aber nicht, ob sie zugelassen oder blockiert werden soll. Dies ist eine Aktion, die nicht beendet wird. AWS WAF setzt die Verarbeitung der verbleibenden Regeln in der Web-ACL fort. In von Ihnen definierten Regeln können Sie benutzerdefinierte Header in die Anforderung einfügen und Labels hinzufügen, mit denen andere Regeln übereinstimmen können.
- **CAPTCHA und Challenge** — AWS WAF verwendet CAPTCHA-Rätsel und stille Challenges, um zu überprüfen, ob die Anfrage nicht von einem Bot stammt, und AWS WAF verwendet Tokens, um die letzten erfolgreichen Kundenantworten nachzuverfolgen.

Note

Ihnen werden zusätzliche Gebühren berechnet, wenn Sie die Aktion CAPTCHA oder die Challenge Regel in einer Ihrer Regeln oder als Überschreibung von Regelaktionen in einer Regelgruppe verwenden. Weitere Informationen finden Sie unter [AWS WAF - Preisgestaltung](#).

Diese Regelaktionen können abhängig vom Status des Tokens in der Anfrage beendet oder nicht beendet werden:

- **Nicht terminierend für ein gültiges, nicht abgelaufenes Token** — Wenn das Token gemäß dem konfigurierten CAPTCHA oder der Challenge-Immunitätszeit gültig und nicht abgelaufen ist, wird die Anfrage ähnlich wie die Aktion behandelt. AWS WAF Count AWS WAF überprüft die Webanforderung weiterhin auf der Grundlage der verbleibenden Regeln in der Web-ACL. Ähnlich wie bei der Count Konfiguration können Sie in Regeln, die Sie definieren, diese Aktionen optional mit benutzerdefinierten Headern konfigurieren, die in die Anfrage eingefügt werden, und Sie können Labels hinzufügen, mit denen andere Regeln übereinstimmen können.
- **Beenden mit blockierter Anfrage für ein ungültiges oder abgelaufenes Token** — Wenn das Token ungültig ist oder der angegebene Zeitstempel abgelaufen ist, wird die Überprüfung der Webanforderung AWS WAF beendet und die Anfrage blockiert, ähnlich wie bei der Aktion. Block AWS WAF antwortet dem Client dann mit einem benutzerdefinierten Antwortcode. Denn CAPTCHA wenn der Inhalt der Anfrage darauf hindeutet, dass der Client-Browser damit umgehen kann, AWS WAF sendet er ein CAPTCHA-Puzzle in einem JavaScript Interstitial, das menschliche Kunden von Bots unterscheiden soll. Für die Challenge Aktion wird ein JavaScript Interstitial mit einer stillen Aufforderung AWS WAF gesendet, mit der normale Browser von Sitzungen unterschieden werden sollen, die von Bots ausgeführt werden.

Weitere Informationen finden Sie unter [CAPTCHA und Challenge in AWS WAF](#).

Informationen zur Verwendung dieser Option finden Sie unter [Regelaktionen in einer Regelgruppe überschreiben](#).

Überschreiben der Regelaktion an Count

Der häufigste Anwendungsfall für das Außerkraftsetzen von Regelaktionen ist das Überschreiben einiger oder aller RegelaktionenCount, um das Verhalten einer Regelgruppe zu testen und zu überwachen, bevor sie in Betrieb genommen wird.

Sie können dies auch verwenden, um Fehler bei einer Regelgruppe zu beheben, die Fehlalarme generiert. Falsch positive Ergebnisse treten auf, wenn eine Regelgruppe Datenverkehr blockiert, von dem Sie nicht erwarten, dass er blockiert wird. Wenn Sie innerhalb einer Regelgruppe eine Regel identifizieren, die Anfragen blockiert, die Sie zulassen möchten, können Sie die Anzahl der Aktionen für diese Regel außer Kraft setzen, um sie von der Bearbeitung Ihrer Anfragen auszuschließen.

Weitere Informationen zur Verwendung der Überschreibung von Regelaktionen beim Testen finden Sie unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

JSON-Liste: **RuleActionOverrides** ersetzt **ExcludedRules**

Wenn Sie Count in Ihrer Web-ACL-Konfiguration vor dem 27. Oktober 2022 Regelaktionen für Regelgruppen auf festgelegt AWS WAF haben, haben Sie Ihre Überschreibungen in der Web-ACL-JSON unter gespeichert. `ExcludedRules` Die JSON-Einstellung für das Überschreiben einer Regel Count befindet sich jetzt in den `RuleActionOverrides` Einstellungen.

Wenn Sie die AWS WAF Konsole verwenden, um die vorhandenen Regelgruppeneinstellungen zu bearbeiten, konvertiert die Konsole automatisch alle `ExcludedRules` Einstellungen im JSON in `RuleActionOverrides` Einstellungen, wobei die Aktion „Überschreiben“ auf Count gesetzt ist.

- Beispiel für eine aktuelle Einstellung:

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

]

- Beispiel für eine alte Einstellung:

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

Wir empfehlen Ihnen, alle `ExcludedRules` Einstellungen in Ihren JSON-Einträgen auf `RuleActionOverrides` Einstellungen zu aktualisieren, bei denen die Aktion auf `isCount` eingestellt ist. Die API akzeptiert beide Einstellungen, aber Sie erhalten Konsistenz in Ihren JSON-Auflistungen zwischen Ihrer Konsolenarbeit und Ihrer API-Arbeit, wenn Sie nur die neue `RuleActionOverrides` Einstellung verwenden.

Aktion der Regelgruppe überschreiben zu `Count`

Sie können die Aktion, die die Regelgruppe zurückgibt, überschreiben, indem Sie sie auf `setCount` festlegen.

Note

Dies ist keine gute Option, um die Regeln in einer Regelgruppe zu testen, da sie nichts daran ändert, wie die Regelgruppe selbst von AWS WAF ausgewertet wird. Es wirkt sich nur darauf aus, wie AWS WAF mit Ergebnissen umgegangen wird, die aus der Regelgruppenauswertung an die Web-ACL zurückgegeben werden. Wenn Sie die Regeln einer Regelgruppe testen möchten, gehen Sie wie im vorherigen Abschnitt ([Regelaktionen überschreiben](#)) beschrieben vor.

Wenn Sie die Regelgruppenaktion auf `setCount` überschreiben, wird die Regelgruppenauswertung normal von AWS WAF verarbeitet.

Wenn keine Regeln in der Regelgruppe übereinstimmen oder wenn alle übereinstimmenden Regeln eine Count Aktion haben, hat diese Überschreibung keine Auswirkung auf die Verarbeitung der Regelgruppe oder der Web-ACL.

Die erste Regel in der Regelgruppe, die einer Webanforderung entspricht und über eine abschließende Regelaktion verfügt, führt AWS WAF dazu, dass die Auswertung der Regelgruppe beendet wird und das Ergebnis der beendenden Aktion an die Web-ACL-Evaluierungsebene zurückgegeben wird. Zu diesem Zeitpunkt, bei der Web-ACL-Evaluierung, wird diese Überschreibung wirksam. AWS WAF setzt die abschließende Aktion außer Kraft, sodass das Ergebnis der Regelgruppenauswertung nur eine Count Aktion ist. AWS WAF setzt dann die Verarbeitung der restlichen Regeln in der Web-ACL fort.

Informationen zur Verwendung dieser Option finden Sie unter [Das Auswertungsergebnis einer Regelgruppe überschreiben in Count](#).

Die Web-ACL-Standardaktion

Wenn Sie eine Web-ACL erstellen und konfigurieren, müssen Sie die Web-ACL-Standardaktion festlegen. AWS WAF wendet diese Aktion auf jede Webanforderung an, die alle Regelauswertungen der Web-ACL durchläuft, ohne dass eine abschließende Aktion auf sie angewendet wird. Eine abschließende Aktion stoppt die Web-ACL-Auswertung der Anfrage und lässt sie entweder an Ihre geschützte Anwendung weiterleiten oder blockiert sie. Hinweise zu Regelaktionen finden Sie unter [Regelaktion](#).

Die Standardaktion der Web-ACL muss die endgültige Disposition der Webanforderung bestimmen, es handelt sich also um eine abschließende Aktion:

- **Allow**— Wenn Sie den meisten Benutzern den Zugriff auf Ihre Website ermöglichen möchten, Sie aber den Zugriff von Angreifern blockieren möchten, deren Anfragen von bestimmten IP-Adressen stammen oder deren Anfragen bösartigen SQL-Code oder bestimmte Werte zu enthalten scheinen, wählen Sie Allow die Standardaktion. Wenn Sie dann Regeln zu Ihrer Web-ACL hinzufügen, fügen Sie Regeln hinzu, die die spezifischen Anforderungen identifizieren und blockieren, die Sie blockieren möchten. Mit dieser Aktion können Sie benutzerdefinierte Header in die Anforderung einfügen, bevor Sie sie an die geschützte Ressource weiterleiten.
- **Block**— Wenn Sie verhindern möchten, dass die meisten Benutzer auf Ihre Website zugreifen, Sie aber Benutzern Zugriff gewähren möchten, deren Anfragen von bestimmten IP-Adressen stammen oder deren Anfragen bestimmte Werte enthalten, wählen Sie Block die Standardaktion. Wenn Sie dann Regeln zu Ihrer Web-ACL hinzufügen, fügen Sie Regeln hinzu, die die spezifischen Anforderungen identifizieren und zulassen, die Sie zulassen möchten. Standardmäßig antwortet die

AWS Ressource für die Block Aktion mit einem 403 (Forbidden) HTTP-Statuscode, aber Sie können die Antwort anpassen.

Informationen zum Anpassen von Anforderungen und Antworten finden Sie unter [Benutzerdefinierte Webanforderungen und Antworten in AWS WAF](#).

Die Konfiguration Ihrer eigenen Regeln und Regelgruppen hängt zum Teil davon ab, ob Sie die meisten Webanforderungen zulassen oder blockieren möchten. Wenn Sie beispielsweise die meisten Anfragen zulassen möchten, setzen Sie die Web-ACL-Standardaktion auf und fügen dann Regeln hinzuAllow, die Webanfragen identifizieren, die Sie blockieren möchten, wie die folgenden:

- Anforderungen, die von IP-Adressen stammen, die eine übermäßige Anzahl von Anforderungen senden
- Anfragen, die aus Ländern stammen, in denen Sie keine Geschäfte tätigen oder die häufige Quelle von Angriffen sind
- Anforderungen mit gefälschten Werten im User-agent-Header
- Anforderungen, die anscheinend schädlichen SQL-Code enthalten

In den Regeln für verwaltete Regelgruppen wird die Block Aktion normalerweise verwendet, aber nicht alle. Beispielsweise verwenden einige Regeln, die für die Bot-Kontrolle verwendet werden, die Challenge Aktionseinstellungen CAPTCHA und. Informationen zu verwalteten Regelgruppen finden Sie unter [Verwaltete Regelgruppen](#).

Verwaltung der Größenbeschränkungen bei Körperinspektionen

Die Größenbeschränkung für Karosserieinspektionen ist die maximale Körpergröße, die auf Anfrage geprüft AWS WAF werden kann. Wenn der Hauptteil einer Webanfrage den Grenzwert überschreitet, leitet der zugrunde liegende Hostdienst nur die Inhalte, die innerhalb des Grenzwerts liegen, AWS WAF zur Inspektion weiter.

- Für Application Load Balancer und AWS AppSync ist das Limit auf 8 KB (8.192 Byte) festgelegt.
- Für CloudFront API Gateway, Amazon Cognito, App Runner und Verified Access beträgt das Standardlimit 16 KB (16.384 Byte), und Sie können das Limit für jeden Ressourcentyp um 16 KB auf bis zu 64 KB erhöhen. Die Einstellungsoptionen sind 16 KB, 32 KB, 48 KB und 64 KB.

Umgang mit übergroßen Körpern

Wenn Ihr Web-Traffic Textkörper umfasst, die das Limit überschreiten, gilt die von Ihnen konfigurierte Handhabung übergroßer Datenmengen. Informationen zu den Optionen für die Bearbeitung von Übergrößen finden Sie unter [Umgang mit übergroßen Webanforderungskomponenten in AWS WAF](#)

Überlegungen zur Preisgestaltung bei Limiterhöhungen

AWS WAF berechnet einen Basistarif für die Überprüfung des Datenverkehrs, der innerhalb des Standardlimits für den Ressourcentyp liegt.

Wenn Sie die Limiteinstellung für CloudFront API Gateway-, Amazon Cognito-, App Runner- und Verified Access-Ressourcen erhöhen, umfasst der Datenverkehr, der untersucht AWS WAF werden kann, Körpergrößen bis zu Ihrem neuen Limit. Nur für die Prüfung von Anfragen, deren Textgröße über den standardmäßigen 16 KB liegt, wird Ihnen ein Aufpreis berechnet. Weitere Informationen über die Preise finden Sie unter [AWS WAF – Preise](#).

Wie ändere ich die Größenbeschränkung für die Karosserieinspektion

Sie können die Größenbeschränkung für die Körperinspektion für CloudFront API Gateway-, Amazon Cognito-, App Runner- oder Verified Access-Ressourcen konfigurieren.

Wenn Sie eine Web-ACL erstellen oder bearbeiten, können Sie die Größenbeschränkungen für die Körperinspektion in der Konfiguration der Ressourcenzuweisung ändern. Informationen zur API finden Sie in der Zuordnungskonfiguration der Web-ACL unter [AssociationConfig](#). Informationen zur Konsole finden Sie in der Konfiguration auf der Seite, auf der Sie die der Web-ACL zugewiesenen Ressourcen angeben. Hinweise zur Konfiguration der Konsole finden Sie unter [Arbeiten mit Web-ACLs](#).

CAPTCHA-, Challenge- und Token-Domain-Konfiguration für eine Web-ACL

Sie können in Ihrer Web-ACL Optionen für die Regeln konfigurieren, die die Challenge Regelaktionen CAPTCHA oder verwenden, und für die Anwendungsintegrations-SDKs, die unbeaufsichtigte Client-Abfragen für AWS WAF verwaltete Schutzmaßnahmen verwalten.

Diese Funktionen reduzieren Bot-Aktivitäten, indem sie Endbenutzer mit CAPTCHA-Rätseln herausfordern und Kundensitzungen vor unbemerkte Herausforderungen stellen. Wenn der Kunde erfolgreich reagiert, AWS WAF stellt er ihm ein Token zur Verfügung, das er in seiner Webanfrage verwenden kann. Dieser ist mit dem Zeitstempel der letzten erfolgreichen Rätsel- und Challenge-Antworten versehen. Weitere Informationen finden Sie unter [AWS WAF intelligente Bedrohungsabwehr](#).

In Ihrer Web-ACL-Konfiguration können Sie konfigurieren, wie diese Token AWS WAF verwaltet werden:

- CAPTCHA- und Challenge-Immunitätszeiten — Diese geben an, wie lange ein CAPTCHA oder ein Challenge-Zeitstempel gültig bleibt. Die Web-ACL-Einstellungen werden von allen Regeln übernommen, für die keine eigenen Immunitätszeiteinstellungen konfiguriert sind, sowie von den Anwendungsintegrations-SDKs. Weitere Informationen finden Sie unter [Ablauf des Zeitstempels: Zeiten der Token-Immunität](#).
- Token-Domänen — AWS WAF akzeptiert standardmäßig nur Token für die Domain der Ressource, der die Web-ACL zugeordnet ist. Wenn Sie eine Token-Domainliste konfigurieren, akzeptiert AWS WAF Tokens für alle Domänen in der Liste und für die Domäne der zugehörigen Ressource. Weitere Informationen finden Sie unter [Konfiguration der Domainliste für Web-ACL-Tokens](#).

Arbeiten mit Web-ACLs

Dieser Abschnitt enthält Verfahren zum Erstellen, Verwalten und Verwenden von Web-ACLs über die AWS Konsole.

Für jede Web-ACL, die Sie verwenden, können Sie auf der Seite der Web-ACL in der AWS WAF Konsole auf der Registerkarte Traffic-Übersicht auf Zusammenfassungen der Web-Traffic-Metriken zugreifen. Die Konsolen-Dashboards bieten fast in Echtzeit Zusammenfassungen der CloudWatch Amazon-Metriken, die bei der Auswertung des Web-Traffics Ihrer Anwendung AWS WAF erfasst werden. Weitere Informationen zu den Dashboards finden Sie unter [Dashboards zur Übersicht über den Web-ACL-Verkehr](#) Weitere Informationen zur Überwachung des Datenverkehrs Ihrer Web-ACL finden Sie unter [Überwachung und Tuning](#).

Risiken rund um Produktionsdatenverkehr

Bevor Sie Änderungen an Ihrer Web-ACL für den Produktionsdatenverkehr implementieren, sollten Sie diese in einer Staging- oder Testumgebung testen und anpassen, bis Sie mit den möglichen Auswirkungen auf Ihren Datenverkehr zufrieden sind. Testen und optimieren Sie anschließend Ihre aktualisierten Regeln im Zählmodus mit Ihrem Produktionsdatenverkehr, bevor Sie sie aktivieren. Anleitungen finden Sie unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

Note

Bei der Verwendung von mehr als 1.500 WCUs in einer Web-ACL fallen Kosten an, die über den Grundpreis für Web-ACL hinausgehen. Weitere Informationen finden Sie unter [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#) und [Preise zu AWS WAF](#).

Temporäre Inkonsistenzen bei Updates

Wenn Sie eine Web-ACL oder andere AWS WAF Ressourcen erstellen oder ändern, dauert es nicht lange, bis die Änderungen in allen Bereichen, in denen die Ressourcen gespeichert sind, übernommen werden. Die Übertragungszeit kann zwischen einigen Sekunden und mehreren Minuten liegen.

Im Folgenden finden Sie Beispiele für temporäre Inkonsistenzen, die Ihnen bei der Übertragung von Änderungen möglicherweise auffallen:

- Wenn Sie nach der Erstellung einer Web-ACL versuchen, sie einer Ressource zuzuordnen, wird möglicherweise eine Ausnahme angezeigt, die darauf hinweist, dass die Web-ACL nicht verfügbar ist.
- Nachdem Sie einer Web-ACL eine Regelgruppe hinzugefügt haben, gelten die neuen Regelgruppenregeln möglicherweise in einem Bereich, in dem die Web-ACL verwendet wird, und nicht in einem anderen.
- Nachdem Sie eine Regelaktionseinstellung geändert haben, sehen Sie möglicherweise an einigen Stellen die alte Aktion und an anderen die neue Aktion.
- Nachdem Sie einem IP-Set, das in einer Sperrregel verwendet wird, eine IP-Adresse hinzugefügt haben, wird die neue Adresse möglicherweise in einem Bereich blockiert, während sie in einem anderen weiterhin zulässig ist.

Themen

- [Erstellen einer Web-ACL](#)
- [Bearbeiten einer Web-ACL](#)
- [Verwaltung des Verhaltens von Regelgruppen in einer Web-ACL](#)
- [Zuordnen oder Aufheben der Zuordnung einer Web-ACL zu einer Ressource AWS](#)
- [Löschen einer Web-ACL](#)

Erstellen einer Web-ACL

Um eine neue Web-ACL zu erstellen, verwenden Sie den Assistenten zum Erstellen von Web-ACLs gemäß dem Verfahren auf dieser Seite.

Risiken rund um Produktionsdatenverkehr

Bevor Sie Änderungen an Ihrer Web-ACL für den Produktionsdatenverkehr implementieren, sollten Sie diese in einer Staging- oder Testumgebung testen und anpassen, bis Sie mit den möglichen Auswirkungen auf Ihren Datenverkehr zufrieden sind. Testen und optimieren Sie anschließend Ihre aktualisierten Regeln im Zählmodus mit Ihrem Produktionsdatenverkehr, bevor Sie sie aktivieren. Anleitungen finden Sie unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

Note

Bei der Verwendung von mehr als 1.500 WCUs in einer Web-ACL fallen Kosten an, die über den Grundpreis für Web-ACL hinausgehen. Weitere Informationen finden Sie unter [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#) und [Preise zu AWS WAF](#).

So erstellen Sie eine Web-ACL


1. [Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter `https://console.aws.amazon.com/wafv2/`.](#)
2. Wählen Sie im Navigationsbereich Web ACLs (Web-ACLs) und dann Create web ACL (Web-ACL erstellen).
3. Geben Sie unter Name den Namen ein, mit dem Sie diese Web-ACL bezeichnen möchten.

Note

Sie können den Namen nach dem Erstellen der Web-ACL nicht mehr ändern.

4. (Optional) Geben Sie für Description - optional (Beschreibung–optional) eine längere Beschreibung für die Web-ACL ein, wenn Sie möchten.
5. Ändern Sie für den CloudWatch Metrikenamen gegebenenfalls den Standardnamen. Befolgen Sie die Anweisungen zu gültigen Zeichen in der Konsole. Der Name darf keine Sonderzeichen,

Leerzeichen oder Metriknamen enthalten, für die reserviert ist AWS WAF, einschließlich „All“ und „Default_Action“.

 Note

Sie können den CloudWatch Metriknamen nicht mehr ändern, nachdem Sie die Web-ACL erstellt haben.

6. Wählen Sie unter Ressourcentyp die AWS Ressourcenkategorie aus, die Sie dieser Web-ACL zuordnen möchten, entweder CloudFront Amazon-Distributionen oder Regionale Ressourcen. Weitere Informationen finden Sie unter [Zuordnen oder Aufheben der Zuordnung einer Web-ACL zu einer Ressource AWS](#).
7. Wenn Sie einen regionalen Ressourcentyp ausgewählt haben, wählen Sie unter Region die Region aus, in der Sie die Web-ACL speichern AWS WAF möchten.

Sie müssen diese Option nur für regionale Ressourcentypen auswählen. Bei CloudFront Distributionen ist die Region fest auf die Region USA Ost (Nord-Virginia) codiertus-east-1, für globale (CloudFront) Anwendungen.
8. (CloudFront, API Gateway, Amazon Cognito, App Runner und Verified Access) Für Inspektionsgrößenbeschränkungen für Webanfragen — optional, wenn Sie eine andere Größenbeschränkung für die Karosserieinspektion angeben möchten, wählen Sie die Obergrenze aus. Bei der Inspektion von Körpergrößen über dem Standardwert von 16 KB können zusätzliche Kosten anfallen. Weitere Informationen zu dieser Option finden Sie unter [Verwaltung der Größenbeschränkungen bei Körperinspektionen](#).
9. (Optional) Wählen Sie unter Zugeordnete AWS Ressourcen — optional, wenn Sie Ihre Ressourcen jetzt angeben möchten, die Option Ressourcen hinzufügen AWS aus. Wählen Sie im Dialogfeld die Ressourcen aus, die Sie zuordnen möchten, und klicken Sie dann auf Hinzufügen. AWS WAF kehrt zur Seite „Web-ACL und zugehörige AWS Ressourcen beschreiben“ zurück.
10. Wählen Sie Weiter aus.
11. (Optional) Wenn Sie verwaltete Regelgruppen hinzufügen möchten, wählen Sie auf der Seite Add rules and rule groups (Regeln und Regelgruppen) Add rules (Regeln hinzufügen) aus. Wählen Sie dann Add managed rule groups (Verwaltete Regelgruppen hinzufügen) aus. Führen Sie die folgenden Schritte für jede verwaltete Regelgruppe aus, die Sie hinzufügen möchten:
 - a. Erweitern Sie auf der Seite Verwaltete Regelgruppen hinzufügen das Angebot für AWS verwaltete Regelgruppen oder für den AWS Marketplace Verkäufer Ihrer Wahl.

- b. Aktivieren Sie für die Regelgruppe, die Sie hinzufügen möchten, in der Spalte Aktion die Option Zur Web-ACL hinzufügen.


Um anzupassen, wie Ihre Web-ACL die Regelgruppe verwendet, wählen Sie Bearbeiten. Im Folgenden finden Sie allgemeine Anpassungseinstellungen:

- Überschreiben Sie die Regelaktionen für einige oder alle Regeln. Wenn Sie keine Aktion zum Außerkraftsetzen für eine Regel definieren, verwendet die Auswertung die Regelaktion, die innerhalb der Regelgruppe definiert ist. Weitere Informationen zu dieser Option finden Sie unter [Aktionsüberschreibungen in Regelgruppen](#).
- Reduzieren Sie den Umfang der Webanfragen, die von der Regelgruppe geprüft werden, indem Sie eine Scopedown-Anweisung hinzufügen. Weitere Informationen zu dieser Option finden Sie unter [Eingrenzungsanweisungen](#).
- Bei einigen verwalteten Regelgruppen müssen Sie zusätzliche Konfigurationen angeben. Weitere Informationen finden Sie in der Dokumentation Ihres Anbieters für verwaltete Regelgruppen. Spezifische Informationen zu den Regelgruppen für AWS verwaltete Regeln finden Sie unter [AWS Verwaltete Regeln für AWS WAF](#).

Wenn Sie mit Ihren Einstellungen fertig sind, wählen Sie Regel speichern.


Wählen Sie Add rules (Regeln hinzufügen), um das Hinzufügen verwalteter Regeln abzuschließen und zur Seite Add rules and rule groups (Regeln und Regelgruppen hinzufügen) zurückzukehren.

12. (Optional) Wenn Sie Ihre eigene Regelgruppe hinzufügen möchten, wählen Sie auf der Seite Add rules and rule groups (Regeln und Regelgruppen) Add rules (Regeln hinzufügen). Aus wählen Sie dann Add my own rules and rule groups (Eigene Regeln und Regelgruppen hinzufügen) aus. Führen Sie die folgenden Schritte für jede Regelgruppe aus, die Sie hinzufügen möchten:
 - a. Wählen Sie auf der Seite Add my own rules and rule groups (Eigene Regeln und Regelgruppen hinzufügen) Rule group (Regelgruppe).
 - b. Geben Sie unter Name den Namen ein, den Sie für die Regelgruppenregel in dieser Web-ACL verwenden möchten. Verwenden Sie keine Namen, die mitAWS, ShieldPreFM, oder beginnenPostFM. Diese Zeichenfolgen sind entweder reserviert oder könnten zu Verwechslungen mit Regelgruppen führen, die von anderen Diensten für Sie verwaltet werden. Siehe [Regelgruppen, die von anderen Services bereitgestellt werden](#).
 - c. Wählen Sie Ihre Regelgruppe aus der Liste aus.

 Note

Wenn Sie die Regelaktionen für eine eigene Regelgruppe überschreiben möchten, speichern Sie sie zunächst in der Web-ACL und bearbeiten Sie dann die Web-ACL und die Regelgruppen-Referenzanweisung in der Regelliste der Web-ACL. Sie können die Regelaktionen mit jeder gültigen Aktionseinstellung überschreiben, genauso wie Sie es für verwaltete Regelgruppen tun können.


- d. Wählen Sie Regel hinzufügen aus.
13. (Optional) Wenn Sie Ihre eigene Regelgruppe hinzufügen möchten, wählen Sie auf der Seite Add rules and rule groups (Regeln und Regelgruppen) Add rules (Regeln hinzufügen). Aus wählen Sie dann Add my own rules and rule groups (Eigene Regeln und Regelgruppen hinzufügen), Rule builder (Rule-Builder) und Rule visual editor (Visueller Regeleditor) aus.

 Note

Der Visuelle Regel-Editor der Konsole unterstützt eine Verschachtelungsebene. Beispielsweise können Sie eine einzelne logische AND- oder OR-Anweisung verwenden und eine Ebene anderer Anweisungen darin verschachteln. Sie können logische Anweisungen jedoch nicht innerhalb logischer Anweisungen verschachteln. Um komplexere Regelanweisungen zu verwalten, verwenden Sie den JSON-Regel-Editor. Informationen zu allen Optionen für Regeln finden Sie unter [AWS WAF Regeln](#). Diese Prozedur deckt den Visuellen Regel-Editor ab.

- a. Geben Sie unter Name den Namen ein, mit dem Sie diese Regel bezeichnen möchten. Verwenden Sie keine Namen, die mit `AWS`, `ShieldPreFM`, oder `beginnenPostFM` beginnen. Diese Zeichenfolgen sind entweder reserviert oder könnten zu Verwechslungen mit Regelgruppen führen, die von anderen Diensten für Sie verwaltet werden.
- b. Geben Sie Ihre Regeldefinition entsprechend Ihren Anforderungen ein. Sie können Regeln innerhalb von logischen AND- und OR-Regelanweisungen kombinieren. Der Assistent führt Sie je nach Kontext durch die Optionen der einzelnen Regeln. Informationen zu den Optionen Ihrer Regeln finden Sie unter [AWS WAF Regeln](#).
- c. Wählen Sie unter Action (Aktion) die Aktion aus, die die Regel ausführen soll, wenn sie einer Webanforderung entspricht. Informationen zu Ihren Auswahlmöglichkeiten finden Sie unter [Regelaktion](#) und [Auswertung von Web-ACL-Regeln und -Regelgruppen](#).

Wenn Sie die ChallengeAktion CAPTCHA oder verwenden, passen Sie die Konfiguration der Immunitätszeit nach Bedarf für die Regel an. Wenn Sie die Einstellung nicht angeben, erbt die Regel sie von der Web-ACL. Um die Einstellungen für die Immunitätszeit der Web-ACL zu ändern, bearbeiten Sie die Web-ACL, nachdem Sie sie erstellt haben. Weitere Hinweise zu Immunitätszeiten finden Sie unter [Ablauf des Zeitstempels: Zeiten der Token-Immunität](#).

 Note

Ihnen werden zusätzliche Gebühren berechnet, wenn Sie die Challenge Regelaktion CAPTCHA oder in einer Ihrer Regeln oder als Überschreibung von Regelaktionen in einer Regelgruppe verwenden. Weitere Informationen finden Sie unter [AWS WAF - Preisgestaltung](#).

Wenn Sie die Anfrage oder Antwort anpassen möchten, wählen Sie die Optionen dafür aus und geben Sie die Details der Anpassung ein. Weitere Informationen finden Sie unter [Benutzerdefinierte Webanforderungen und Antworten in AWS WAF](#).

Wenn Sie möchten, dass Ihre Regel Kennzeichnungen zu übereinstimmenden Webanforderungen hinzufügt, wählen Sie die Optionen dafür aus und geben Sie die Kennzeichnungsdetails ein. Weitere Informationen finden Sie unter [AWS WAF Labels auf Webanfragen](#).

d. Wählen Sie Regel hinzufügen aus.

14. Wählen Sie die Standardaktion für die Web-ACL, entweder Block oder Allow. Dies ist die Aktion, die AWS WAF bei einer Anfrage ausgeführt wird, wenn die Regeln in der Web-ACL sie nicht explizit zulassen oder blockieren. Weitere Informationen finden Sie unter [Die Web-ACL-Standardaktion](#).

Wenn Sie die Standardaktion anpassen möchten, wählen Sie die Optionen dafür aus und geben Sie die Details der Anpassung ein. Weitere Informationen finden Sie unter [Benutzerdefinierte Webanforderungen und Antworten in AWS WAF](#).

15. Sie können eine Token-Domainliste definieren, um die gemeinsame Nutzung von Token zwischen geschützten Anwendungen zu ermöglichen. Tokens werden von den Challenge Aktionen CAPTCHA und von den SDKs für die Anwendungsintegration verwendet, die Sie implementieren, wenn Sie die Regelgruppen mit AWS verwalteten Regeln für die Erstellung

von Konten zur AWS WAF Betrugsbekämpfung, zur Betrugsprävention (ACFP), AWS WAF zur Verhinderung von Kontoübernahmen (ATP) und zur AWS WAF Bot-Kontrolle verwenden.

Öffentliche Suffixe sind nicht zulässig. Beispielsweise können Sie gov . au oder nicht co . uk als Token-Domain verwenden.

AWS WAF Akzeptiert standardmäßig nur Token für die Domäne der geschützten Ressource. Wenn Sie Tokendomänen zu dieser Liste hinzufügen, AWS WAF akzeptiert Tokens für alle Domänen in der Liste und für die Domäne der zugehörigen Ressource. Weitere Informationen finden Sie unter [Konfiguration der Domainliste für Web-ACL-Tokens](#).

16. Wählen Sie Weiter.
17. Wählen Sie auf der Seite Regelpriorität festlegen Ihre Regeln und Regelgruppen aus und verschieben Sie sie in die Reihenfolge, in der Sie sie verarbeiten AWS WAF möchten. AWS WAF verarbeitet Regeln, beginnend am Anfang der Liste. Wenn Sie die Web-ACL speichern, weist AWS WAF den Regeln in der Reihenfolge numerische Prioritätseinstellungen zu, in der Sie sie aufgeführt haben. Weitere Informationen finden Sie unter [Reihenfolge der Verarbeitung von Regeln und Regelgruppen in einer Web-ACL](#).
18. Wählen Sie Weiter.
19. Sehen Sie sich die Optionen auf der Seite Configure metrics (Metriken konfigurieren) an und nehmen Sie alle erforderlichen Änderungen vor. Sie können Metriken aus mehreren Quellen kombinieren, indem Sie denselben CloudWatch Metrikenamen für sie angeben.
20. Wählen Sie Weiter aus.
21. Überprüfen Sie auf der Seite Review and create web ACL (Überprüfen und Web-ACL erstellen) Ihre Definitionen. Wenn Sie einen Bereich ändern möchten, wählen Sie Edit (Bearbeiten) für den Bereich. Dadurch kehren Sie zur Seite im Web-ACL-Assistenten zurück. Nehmen Sie alle Änderungen vor und wählen Sie dann Next (Weiter), bis Sie zur Seite Review and create web ACL (Überprüfen und Web-ACL erstellen) zurückkehren.
22. Wählen Sie Create web ACL (Web-ACL erstellen) aus. Ihre neue Web-ACL wird auf der Seite Web-ACLs aufgelistet.

Bearbeiten einer Web-ACL

Um Regeln zu einer Web-ACL hinzuzufügen oder zu entfernen oder Konfigurationseinstellungen zu ändern, greifen Sie wie auf dieser Seite beschrieben auf die Web-ACL zu. Bei der Aktualisierung einer Web-ACL AWS WAF werden die Ressourcen, die Sie mit der Web-ACL verknüpft haben, kontinuierlich abgedeckt.

Risiken rund um Produktionsdatenverkehr

Bevor Sie Änderungen an Ihrer Web-ACL für den Produktionsdatenverkehr implementieren, sollten Sie diese in einer Staging- oder Testumgebung testen und anpassen, bis Sie mit den möglichen Auswirkungen auf Ihren Datenverkehr zufrieden sind. Testen und optimieren Sie anschließend Ihre aktualisierten Regeln im Zählmodus mit Ihrem Produktionsdatenverkehr, bevor Sie sie aktivieren. Anleitungen finden Sie unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

Note

Bei der Verwendung von mehr als 1.500 WCUs in einer Web-ACL fallen Kosten an, die über den Grundpreis für Web-ACL hinausgehen. Weitere Informationen finden Sie unter [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#) und [Preise zu AWS WAF](#).

So bearbeiten Sie eine Web-ACL

1. [Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/).
2. Wählen Sie im Navigationsbereich Web ACLs aus.
3. Wählen Sie den Namen der Web-ACL aus, die Sie bearbeiten möchten. Über die Konsole gelangen Sie zur Beschreibung der Web-ACL.


Note

Web-ACLs, die von verwaltet werden, AWS Firewall Manager haben Namen, die mit FMManagedWebACLV2- beginnen. Der Firewall Manager Manager-Administrator verwaltet diese in den Firewall Manager AWS WAF Manager-Richtlinien. Diese Web-ACLs können Regelgruppensätze enthalten, die für die erste und letzte Ausführung in der Web-ACL auf beiden Seiten von Regeln oder Regelgruppen bestimmt sind, die Sie hinzufügen und verwalten. Sie können keine dieser ersten und letzten Regelgruppenspezifikationen ändern. Die Namen der ersten und letzten Regelgruppe beginnen mit PREFMManaged- bzw. POSTFMManaged-. Weitere Informationen zu diesen Richtlinien finden Sie unter [AWS WAF Richtlinien](#).


4. Bearbeiten Sie die Web-ACL nach Bedarf. Wählen Sie die Registerkarten für die Konfigurationsbereiche aus, die Sie interessieren, und bearbeiten Sie die veränderbaren Einstellungen. Wenn Sie für jede Einstellung, die Sie bearbeiten, auf Speichern klicken und zur Beschreibungsseite der Web-ACL zurückkehren, speichert die Konsole Ihre Änderungen an der Web-ACL.

Im Folgenden werden die Registerkarten aufgeführt, die die Web-ACL-Konfigurationskomponenten enthalten.

- Registerkarte „Regeln“
 - In der Web-ACL definierte Regeln — Sie können die Regeln, die Sie in der Web-ACL definiert haben, ähnlich wie bei der Erstellung der Web-ACL bearbeiten und verwalten.

 Note

Ändern Sie nicht die Namen von Regeln, die Sie Ihrer Web-ACL nicht manuell hinzugefügt haben. Wenn Sie andere Dienste verwenden, um Regeln für Sie zu verwalten, könnte eine Änderung ihrer Namen dazu führen, dass sie nicht mehr oder weniger in der Lage sind, den beabsichtigten Schutz zu bieten. AWS Shield Advanced und AWS Firewall Manager beide erstellen Regeln in Ihrer Web-ACL. Weitere Informationen finden Sie unter [Regelgruppen, die von anderen Services bereitgestellt werden](#).

 Note

Wenn Sie den Namen einer Regel ändern und möchten, dass der Metrikname der Regel die Änderung widerspiegelt, müssen Sie auch den Metriknamen aktualisieren. AWS WAF aktualisiert den Metriknamen für eine Regel nicht automatisch, wenn Sie den Regelnamen ändern. Sie können den Metriknamen ändern, wenn Sie die Regel in der Konsole bearbeiten, indem Sie den JSON-Editor für Regeln verwenden. Sie können beide Namen auch über die APIs und in jeder JSON-Liste ändern, mit der Sie Ihre Web-ACL oder Regelgruppe definieren.

Informationen zu Regeln und Regelgruppeneinstellungen finden Sie unter [AWS WAF Regeln](#) und [Regelgruppen](#).

- **Verwendete Kapazitätseinheiten für Web-ACL-Regeln** — Die aktuelle Kapazitätsnutzung für Ihre Web-ACL. Dies ist nur zur Ansicht vorgesehen.
- **Standard-Web-ACL-Aktion für Anfragen, die keinen Regeln entsprechen** — Informationen zu dieser Einstellung finden Sie unter [Die Web-ACL-Standardaktion](#).
- **Web-ACL-CAPTCHA- und Challenge-Konfigurationen** — Diese Immunitätszeiten bestimmen, wie lange ein CAPTCHA oder ein Challenge-Token nach dem Erwerb gültig bleibt. Sie können diese Einstellung hier nur ändern, nachdem Sie die Web-ACL erstellt haben. Weitere Informationen zu diesen Einstellungen finden Sie unter [Ablauf des Zeitstempels: Zeiten der Token-Immunität](#).
- **Token-Domainliste** — AWS WAF akzeptiert Token für alle Domänen in der Liste und für die Domäne der zugehörigen Ressource. Weitere Informationen finden Sie unter [Konfiguration der Domainliste für Web-ACL-Tokens](#).
- **Registerkarte „AWS Zugeordnete Ressourcen“**
 - **Größenbeschränkung für die Inspektion von Webanfragen** — Nur für Web-ACLs enthalten, die CloudFront Distributionen schützen. Die Größenbeschränkung für die Karosserieinspektion bestimmt, welcher Teil der Karosseriekomponente AWS WAF zur Inspektion weitergeleitet wird. Weitere Informationen zu dieser Einstellung finden Sie unter [Verwaltung der Größenbeschränkungen bei Körperinspektionen](#).
 - **Zugeordnete AWS Ressourcen** — Die Liste der Ressourcen, denen die Web-ACL derzeit zugeordnet ist und die sie schützt. Sie können nach Ressourcen suchen, die sich in derselben Region wie die Web-ACL befinden, und sie der Web-ACL zuordnen. Weitere Informationen finden Sie unter [Zuordnen oder Aufheben der Zuordnung einer Web-ACL zu einer Ressource AWS](#).
- **Registerkarte „Benutzerdefinierte Antworttexte“**
 - **Benutzerdefinierte Antworttextkörper, die von Ihren Web-ACL-Regeln verwendet werden können, für die die Aktion auf festgelegt ist Block**. Weitere Informationen finden Sie unter [Benutzerdefinierte Antworten für Block Aktionen](#).
- **Registerkarte „Protokollierung und Metriken“**
 - **Protokollierung** — Protokollierung des Datenverkehrs, den die Web-ACL auswertet. Weitere Informationen finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).
 - **Stichprobenanfragen** — Informationen zu den Regeln, die Webanfragen entsprechen. Informationen zum Anzeigen von Stichprobenanforderungen finden Sie unter [Anzeigen einer Stichprobe von Webanforderungen](#).

- CloudWatch Metriken — Metriken für die Regeln in Ihrer Web-ACL. Informationen zu CloudWatch Amazon-Metriken finden Sie unter [Überwachung mit Amazon CloudWatch](#).

Temporäre Inkonsistenzen bei Aktualisierungen

Wenn Sie eine Web-ACL oder andere AWS WAF Ressourcen erstellen oder ändern, dauert es nicht lange, bis die Änderungen in allen Bereichen, in denen die Ressourcen gespeichert sind, übernommen werden. Die Übertragungszeit kann zwischen einigen Sekunden und mehreren Minuten liegen.

Im Folgenden finden Sie Beispiele für temporäre Inkonsistenzen, die Ihnen bei der Übertragung von Änderungen möglicherweise auffallen:

- Wenn Sie nach der Erstellung einer Web-ACL versuchen, sie einer Ressource zuzuordnen, wird möglicherweise eine Ausnahme angezeigt, die darauf hinweist, dass die Web-ACL nicht verfügbar ist.
- Nachdem Sie einer Web-ACL eine Regelgruppe hinzugefügt haben, gelten die neuen Regelgruppenregeln möglicherweise in einem Bereich, in dem die Web-ACL verwendet wird, und nicht in einem anderen.
- Nachdem Sie eine Regelaktionseinstellung geändert haben, sehen Sie möglicherweise an einigen Stellen die alte Aktion und an anderen die neue Aktion.
- Nachdem Sie einem IP-Set, das in einer Sperrregel verwendet wird, eine IP-Adresse hinzugefügt haben, wird die neue Adresse möglicherweise in einem Bereich blockiert, während sie in einem anderen weiterhin zulässig ist.

Verwaltung des Verhaltens von Regelgruppen in einer Web-ACL

In diesem Abschnitt werden Ihre Möglichkeiten beschrieben, wie Sie die Verwendung einer Regelgruppe in Ihrer Web-ACL ändern können. Diese Informationen gelten für alle Regelgruppentypen. Nachdem Sie einer Web-ACL eine Regelgruppe hinzugefügt haben, können Sie die Aktionen der einzelnen Regeln in der Regelgruppe durch Count oder durch eine andere gültige Regelaktionseinstellung überschreiben. Sie können auch die resultierende Aktion der Regelgruppe überschreibenCount, was keine Auswirkung darauf hat, wie die Regeln innerhalb der Regelgruppe ausgewertet werden.

Weitere Informationen zu diesen Optionen finden Sie unter [Aktionsüberschreibungen in Regelgruppen](#).

Regelaktionen in einer Regelgruppe überschreiben

Für jede Regelgruppe in einer Web-ACL können Sie die Aktionen der enthaltenen Regel für einige oder alle Regeln überschreiben.

Der häufigste Anwendungsfall hierfür ist das Überschreiben der Regelaktionen, Count um neue oder aktualisierte Regeln zu testen. Wenn Sie Metriken aktiviert haben, erhalten Sie Metriken für jede Regel, die Sie überschreiben. Weitere Informationen zum Testen finden Sie unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

Um Regelaktionen in einer Regelgruppe zu überschreiben

Sie können diese Änderungen vornehmen, wenn Sie der Web-ACL eine verwaltete Regelgruppe hinzufügen, und Sie können sie an jeder Art von Regelgruppe vornehmen, wenn Sie die Web-ACL bearbeiten. Diese Anweisungen gelten für eine Regelgruppe, die bereits zur Web-ACL hinzugefügt wurde. Weitere Informationen zu dieser Option finden Sie unter [Regelaktionen überschreiben](#).

1. Bearbeiten Sie die Web-ACL.
2. Wählen Sie auf der Registerkarte Rules (Regeln) der Web-ACL-Seite die Regelgruppe aus und wählen Sie dann Edit (Bearbeiten).
3. Verwalten Sie im Abschnitt Regeln für die Regelgruppe die Aktionseinstellungen nach Bedarf.
 - Alle Regeln — Um eine Aktion zum Außerkraftsetzen für alle Regeln in der Regelgruppe festzulegen, öffnen Sie das Drop-down-Menü Alle Regelaktionen überschreiben und wählen Sie die Aktion zum Außerkraftsetzen aus. Um die Überschreibungen für alle Regeln zu entfernen, wählen Sie Alle Überschreibungen entfernen aus.
 - Einzelne Regel — Um eine Aktion zum Außerkraftsetzen für eine einzelne Regel festzulegen, öffnen Sie das Drop-down-Menü der Regel und wählen Sie die Aktion zum Außerkraftsetzen aus. Um eine Überschreibung für eine Regel zu entfernen, öffnen Sie das Drop-down-Menü der Regel und wählen Sie Überschreibung entfernen aus.
4. Wenn Sie mit Ihren Änderungen fertig sind, wählen Sie Regel speichern. Die Einstellungen für Regelaktionen und Aktionen zum Außerkraftsetzen sind auf der Regelgruppenseite aufgeführt.

Die folgende JSON-Beispielliste zeigt eine Regelgruppendeklaration in einer Web-ACL, die die Regelaktionen Count für die Regeln CategoryVerifiedSearchEngine und CategoryVerifiedSocialMedia überschreibt. In der JSON-Datei überschreiben Sie alle Regelaktionen, indem Sie für jede einzelne Regel einen RuleActionOverrides Eintrag angeben.


```
{
  "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"
    }
  }
}
```

Das Auswertungsergebnis einer Regelgruppe überschreiben in Count

Sie können die Aktion, die sich aus einer Regelgruppenauswertung ergibt, außer Kraft setzen, ohne die Konfiguration oder Auswertung der Regeln in der Regelgruppe zu ändern. Diese Option wird nicht häufig verwendet. Wenn eine Regel in der Regelgruppe zu einer Übereinstimmung führt, legt diese Überschreibung die resultierende Aktion der Regelgruppe auf festCount.

Note

Dies ist ein ungewöhnlicher Anwendungsfall. Die meisten Aktionsüberschreibungen werden auf Regelebene innerhalb der Regelgruppe vorgenommen, wie unter [beschrieben](#)[Regelaktionen in einer Regelgruppe überschreiben](#).

Sie können die resultierende Aktion der Regelgruppe in der Web-ACL überschreiben, wenn Sie die Regelgruppe hinzufügen oder bearbeiten. Öffnen Sie in der Konsole den optionalen Bereich „Regelgruppe überschreiben“ für die Regelgruppe und aktivieren Sie das Außerkräftsetzen. In der JSON-Datei, die `OverrideAction` in der Regelgruppenanweisung festgelegt ist, wie in der folgenden Beispielliste dargestellt:

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

Zuordnen oder Aufheben der Zuordnung einer Web-ACL zu einer Ressource AWS

Sie können AWS WAF damit die folgenden Verknüpfungen zwischen Web-ACLs und Ihren Ressourcen erstellen:

- Ordnen Sie einer der unten aufgeführten regionalen Ressourcen eine regionale Web-ACL zu. Für diese Option muss sich die Web-ACL in derselben Region wie Ihre Ressource befinden.
 - Amazon API Gateway API-Gateway-REST-API

- Application Load Balancer
 - AWS AppSync GraphQL-API
 - Amazon-Cognito-Benutzerpool
 - AWS App Runner Dienst
 - AWS Instanz mit verifiziertem Zugriff
- Ordnen Sie einer CloudFront Amazon-Distribution eine globale Web-ACL zu. Die globale Web-ACL wird eine fest codierte Region USA Ost (Nord-Virginia) haben.

Sie können einer Distribution auch eine Web-ACL zuordnen, wenn Sie die CloudFront Distribution selbst erstellen oder aktualisieren. Weitere Informationen finden Sie unter [Verwendung AWS WAF zur Steuerung des Zugriffs auf Ihre Inhalte](#) im Amazon CloudFront Developer Guide.

Einschränkungen für mehrere Zuordnungen

Sie können eine einzelne Web-ACL mit einer oder mehreren AWS Ressourcen verknüpfen. Dabei gelten die folgenden Einschränkungen:

- Sie können jede AWS Ressource nur einer Web-ACL zuordnen. Die Beziehung zwischen Web-ACL und AWS Ressourcen ist one-to-many.
- Sie können eine Web-ACL einer oder mehreren CloudFront Distributionen zuordnen. Sie können eine Web-ACL, die Sie einer CloudFront Distribution zugeordnet haben, keinem anderen AWS Ressourcentyp zuordnen.

Zusätzliche Einschränkungen

Die folgenden zusätzlichen Einschränkungen gelten für Web-ACL-Verknüpfungen:

- Sie können eine Web-ACL nur einem Application Load Balancer in AWS-Regionen zuordnen. Es ist beispielsweise nicht möglich, eine Web-ACL einem Application Load Balancer zuzuordnen, der an AWS Outposts ist.
- Sie können einen Amazon Cognito Cognito-Benutzerpool keiner Web-ACL zuordnen, die die verwaltete Regelgruppe AWS WAF Fraud Control Account Creation Fraud Prevention (ACFP) `AWSManagedRulesACFPRuleSet` oder die verwaltete Regelgruppe AWS WAF Fraud Control Account Takeover Prevention (ATP) verwendet. `AWSManagedRulesATPRuleSet` Informationen zur Betrugsprävention bei der Kontoerstellung finden Sie unter [AWS WAF Einrichtung von Konten bei der Betrugsbekämpfung und Betrugsprävention \(ACFP\)](#) Informationen zur Verhinderung

von Kontoübernahmen finden Sie unter [AWS WAF Verhinderung von Kontoübernahmen bei der Betrugsbekämpfung \(ATP\)](#).

⚠ Risiken rund um Produktionsdatenverkehr

Bevor Sie Ihre Web-ACL für den Produktionsdatenverkehr einsetzen, sollten Sie sie in einer Staging- oder Testumgebung testen und optimieren, bis Sie mit den möglichen Auswirkungen auf Ihren Datenverkehr zufrieden sind. Testen und optimieren Sie anschließend Ihre Regeln im Zählmodus mit Ihrem Produktionsdatenverkehr, bevor Sie sie aktivieren. Anleitungen finden Sie unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

Um eine Web-ACL einer AWS Ressource zuzuordnen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich Web ACLs aus.
3. Wählen Sie den Namen der Web-ACL, die Sie mit einer Ressource verknüpfen möchten. Die Konsole führt Sie zur Beschreibung der Web-ACL, wo Sie sie bearbeiten können.
4. Wählen Sie auf der Registerkarte AWS Zugeordnete Ressourcen die Option AWS Ressourcen hinzufügen aus.
5. Wenn Sie dazu aufgefordert werden, wählen Sie den Ressourcentyp aus, aktivieren Sie das Optionsfeld neben der Ressource, die Sie verknüpfen möchten, und klicken Sie dann auf Hinzufügen.

Um die Zuordnung einer Web-ACL zu einer Ressource aufzuheben AWS

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich Web ACLs aus.
3. Wählen Sie den Namen der Web-ACL, die Sie von Ihrer Ressource trennen möchten. Die Konsole führt Sie zur Beschreibung der Web-ACL, wo Sie sie bearbeiten können.
4. Wählen Sie auf der Registerkarte Zugeordnete AWS Ressourcen die Ressource aus, zu der Sie die Zuordnung dieser Web-ACL aufheben möchten.

Note

Sie müssen die Zuordnung zu einer Ressource nach der anderen trennen. Wählen Sie nicht mehrere Ressourcen aus.

5. Wählen Sie Disassociate (Zuordnung aufheben) aus. Die Konsole öffnet einen Bestätigungsdialog. Bestätigen Sie Ihre Entscheidung, die Web-ACL von der AWS Ressource zu trennen.

Löschen einer Web-ACL

Um eine Web-ACL zu löschen, trennen Sie zunächst alle AWS Ressourcen von der Web-ACL. Führen Sie die folgenden Schritte aus.

So löschen Sie eine Web-ACL

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich Web ACLs aus.
3. Wählen Sie den Namen der Web-ACL aus, die Sie löschen möchten. Die Konsole führt Sie zur Beschreibung der Web-ACL, wo Sie sie bearbeiten können.
4. Wählen Sie auf der Registerkarte Zugeordnete AWS Ressourcen für jede zugeordnete Ressource das Optionsfeld neben dem Ressourcennamen aus und klicken Sie dann auf Zuordnung trennen. Dadurch wird die Web-ACL von Ihren AWS Ressourcen getrennt.
5. Wählen Sie im Navigationsbereich Web ACLs aus.
6. Wählen Sie das Optionsfeld neben der Web-ACL, die Sie löschen möchten, und klicken Sie dann auf Delete (Löschen).

Regelgruppen

Eine Regelgruppe ist ein wiederverwendbarer Regelsatz, den Sie zu einer Web-ACL hinzufügen können. Weitere Informationen zu Web-ACLs finden Sie unter [Web-Zugriffskontrolllisten \(Web-ACLs\)](#).

Regelgruppen lassen sich in die folgenden Hauptkategorien einteilen:

- Ihre eigenen Regelgruppen, die Sie erstellen und verwalten.

- Verwaltete Regelgruppen, die von AWS Managed Rules-Teams für Sie erstellt und verwaltet werden.
- Verwaltete Regelgruppen, die AWS Marketplace Verkäufer für Sie erstellen und verwalten.
- Regelgruppen, die anderen Diensten wie Shield Advanced gehören AWS Firewall Manager und von diesen verwaltet werden.

Unterschiede zwischen Regelgruppen und Web-ACLs

Regelgruppen und Web-ACLs enthalten jeweils Regeln, die an beiden Stellen auf die gleiche Weise definiert sind. Regelgruppen unterscheiden sich von Web-ACLs wie folgt:

- Regelgruppen können keine Referenzanweisungen für Regelgruppen enthalten.
- Sie können eine einzelne Regelgruppe in mehreren Web-ACLs wiederverwenden, indem Sie jeder Web-ACL eine Regelgruppenreferenzanweisung hinzufügen. Sie können eine Web-ACL nicht wiederverwenden.
- Regelgruppen haben keine Standardaktionen. In einer Web-ACL legen Sie für jede Regel oder Regelgruppe, die Sie aufnehmen, eine Standardaktion fest. Jede einzelne Regel innerhalb einer Regelgruppe oder Web-ACL hat eine definierte Aktion.
- Sie verknüpfen eine Regelgruppe nicht direkt mit einer AWS Ressource. Um Ressourcen mit einer Regelgruppe zu schützen, verwenden Sie die Regelgruppe in einer Web-ACL.
- Web-ACLs haben eine vom System definierte maximale Kapazität von 5.000 Web-ACL-Kapazitätseinheiten (WCUs). Jede Regelgruppe hat eine WCU-Einstellung, die beim Erstellen festgelegt werden muss. Mit dieser Einstellung können Sie den zusätzlichen Kapazitätsbedarf berechnen, den die Verwendung einer Regelgruppe zu Ihrer Web-ACL hinzufügen würde. Weitere Informationen zu den WCUs finden Sie unter [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#).

Informationen zu Regeln finden Sie unter [AWS WAF Regeln](#).

In diesem Abschnitt finden Sie Anleitungen zur Erstellung und Verwaltung eigener Regelgruppen. Außerdem erfahren Sie mehr über die verwalteten Regelgruppen, die Ihnen zur Verfügung stehen, und darüber, wie Sie diese nutzen.

Themen

- [Verwaltete Regelgruppen](#)
- [Verwaltung Ihrer eigenen Regelgruppen](#)
- [Regelgruppen, die von anderen Services bereitgestellt werden](#)

Verwaltete Regelgruppen

Verwaltete Regelgruppen sind Sammlungen vordefinierter ready-to-use Regeln, die AWS von AWS Marketplace Verkäufern für Sie erstellt und verwaltet werden. AWS WAF Die Grundpreise gelten für Ihre Nutzung jeder verwalteten Regelgruppe. AWS WAF Preisinformationen finden Sie unter [AWS WAF Preisgestaltung](#).

- Die Regelgruppen mit AWS verwalteten Regeln für AWS WAF Bot-Kontrolle, AWS WAF Verhinderung von Kontoübernahmen (ATP) und AWS WAF Fraud Control Account Creation Fraud Prevention (ACFP) sind gegen zusätzliche Gebühren erhältlich, die über die AWS WAF Grundgebühren hinausgehen. Details zu den Preisen finden Sie unter [AWS WAF -Preise](#).
- Alle anderen Regelgruppen für AWS verwaltete Regeln stehen AWS WAF Kunden ohne zusätzliche Kosten zur Verfügung.
- AWS Marketplace verwaltete Regelgruppen sind als Abonnement erhältlich über AWS Marketplace. Jede dieser Regelgruppen gehört dem AWS Marketplace Verkäufer und wird von diesem verwaltet. Preisinformationen für die Verwendung einer AWS Marketplace verwalteten Regelgruppe erhalten Sie vom AWS Marketplace Verkäufer.

Einige verwaltete Regelgruppen wurden entwickelt, um bestimmte Arten von Webanwendungen wie WordPress Joomla oder PHP zu schützen. Andere bieten einen umfassenden Schutz vor bekannten Bedrohungen oder häufigen Schwachstellen von Webanwendungen, beispielsweise einige derjenigen, die in den [OWASP Top 10](#) aufgeführt sind. Wenn Sie Vorschriften wie PCI oder HIPAA unterliegen, können Sie möglicherweise verwaltete Regelgruppen verwenden, um die entsprechenden Anforderungen an die Firewall für Webanwendungen zu erfüllen.

Automatische Updates

Sich über die sich ständig ändernde Bedrohungslandschaft auf dem Laufenden zu halten, kann zeitaufwändig und teuer sein. Mit verwalteten Regelgruppen können Sie Zeit bei der Implementierung und Verwendung AWS WAF sparen. Viele AWS Marketplace Anbieter aktualisieren verwaltete Regelgruppen automatisch und stellen neue Versionen von Regelgruppen bereit, wenn neue Sicherheitslücken und Bedrohungen auftauchen.

In einigen Fällen AWS wird das Unternehmen bereits vor der Veröffentlichung über neue Sicherheitslücken informiert, was auf seine Teilnahme an einer Reihe von privaten Informationsgemeinschaften zurückzuführen ist. In diesen Fällen AWS kann die Regelgruppen für AWS verwaltete Regeln aktualisiert und für Sie bereitgestellt werden, noch bevor eine neue Bedrohung allgemein bekannt wird.

Eingeschränkter Zugriff auf die Regeln in einer verwalteten Regelgruppe

Jede verwaltete Regelgruppe bietet eine umfassende Beschreibung der Arten von Angriffen und Schwachstellen, vor denen sie schützen soll. Um das geistige Eigentum der Regelgruppenanbieter zu schützen, können Sie nicht alle Details der einzelnen Regeln innerhalb einer Regelgruppe einsehen. Diese Einschränkung hilft auch, böswillige Benutzer daran zu hindern, Bedrohungen zu entwerfen, die speziell veröffentlichte Regeln umgehen.

Themen

- [Versionsverwaltung mit verwalteten Regelgruppen](#)
- [Arbeiten mit verwalteten Regelgruppen](#)
- [AWS Verwaltete Regeln für AWS WAF](#)
- [AWS Marketplace verwaltete Regelgruppen](#)

Versionsverwaltung mit verwalteten Regelgruppen

Viele Anbieter verwalteter Regelgruppen aktualisieren die Optionen und Funktionen einer Regelgruppe in neuen Versionen der Regelgruppe. Normalerweise ist eine bestimmte Version einer verwalteten Regelgruppe unverändert. Es kann jedoch gelegentlich vorkommen, dass ein Anbieter einige oder alle seiner vorhandenen Versionen einer verwalteten Regelgruppe aktualisieren muss, etwa um auf eine aufkommende Sicherheitsbedrohung zu reagieren.

Wenn Sie Ihrer Web-ACL eine verwaltete Regelgruppe hinzufügen und diese Regelgruppe die Versionsverwaltung unterstützt, können Sie den Anbieter verwalten lassen, welche Version Sie verwenden, oder die Versionseinstellung selbst verwalten.

Sie können die gewünschte Version nicht finden?

Wenn Sie in der Versionsliste einer Regelgruppe keine Version sehen, ist die Version wahrscheinlich abgelaufen oder sie ist bereits abgelaufen. Wenn für eine Version ein Ablaufdatum geplant ist, können Sie sie nicht AWS WAF mehr für die Regelgruppe auswählen.

Versionierung und SNS-Benachrichtigungen für Regelgruppen mit AWS verwalteten Regeln

Alle Regelgruppen mit AWS verwalteten Regeln bieten Versionsverwaltungs- und SNS-Aktualisierungsbenachrichtigungen, mit Ausnahme der Regelgruppen für IP-Reputation, Bot-Kontrolle und Verhinderung von Kontoübernahmen.

Die Regelgruppen für AWS verwaltete Regeln, die Benachrichtigungen bereitstellen, verwenden alle dasselbe SNS-Thema Amazon Resource Name (ARN).

Themen

- [Versionslebenszyklus für verwaltete Regelgruppen](#)
- [Bewährte Methoden für den Umgang mit Versionen von verwalteten Regelgruppen](#)

Versionslebenszyklus für verwaltete Regelgruppen

Anbieter behandeln die folgenden Lebenszyklusphasen einer statischen Version einer verwalteten Regelgruppe:

- **Veröffentlichung und Updates** — Ein Anbieter verwalteter Regelgruppen kündigt kommende und neue statische Versionen seiner verwalteten Regelgruppen durch Benachrichtigungen zu einem Amazon Simple Notification Service (Amazon SNS) -Thema an. Anbieter können das Thema auch verwenden, um andere wichtige Informationen über ihre Regelgruppen zu kommunizieren, etwa dringend erforderliche Aktualisierungen.

Sie können das Thema der Regelgruppe abonnieren und festlegen, wie Sie Benachrichtigungen erhalten möchten. Weitere Informationen finden Sie unter [Erhalten von Benachrichtigungen zu neuen Versionen und Aktualisierungen](#).

- **Ablaufplanung** – Ein Anbieter von verwalteten Regelgruppen plant, wann ältere Versionen einer Regelgruppe ablaufen. Eine Version, deren Ablauf geplant ist, kann nicht zu Ihren Web-ACL-Regeln hinzugefügt werden. Wenn für eine Version ein Ablauf geplant ist, AWS WAF verfolgt Amazon CloudWatch den Ablauf anhand einer Countdown-Metrik.

Sie können einen Alarm für die Metrik einrichten CloudWatch , um den Ablauf einer Version, die Sie verwenden, zu verfolgen. Dadurch haben Sie Zeit, eine neue Version zu testen und die bisherige Version zu entfernen, bevor sie abgelaufen ist. Weitere Informationen finden Sie unter [Verfolgen des Versionsablaufs](#).

- **Ablauf der Version** — Wenn Sie eine Web-ACL so konfiguriert haben, dass sie eine abgelaufene Version einer verwalteten Regelgruppe verwendet, wird bei der Evaluierung der Web-ACL die Standardversion der Regelgruppe AWS WAF verwendet. AWS WAF Blockiert außerdem alle Aktualisierungen der Web-ACL, die weder die Regelgruppe entfernen noch ihre Version in eine nicht abgelaufene Version ändern.

Wenn Sie AWS Marketplace verwaltete Regelgruppen verwenden, fragen Sie den Anbieter nach weiteren Informationen zu den Versionslebenszyklen.

Bewährte Methoden für den Umgang mit Versionen von verwalteten Regelgruppen

Folgen Sie diesen bewährten Methoden für den Umgang mit der Versionsverwaltung, wenn Sie eine versionierte verwaltete Regelgruppe verwenden.

Wenn Sie eine verwaltete Regelgruppe in Ihrer Web-ACL verwenden, können Sie eine bestimmte unveränderliche Version der Regelgruppe oder die Standardversion verwenden:

- Standardversion — legt als Standardversion AWS WAF immer die statische Version fest, die derzeit vom Anbieter empfohlen wird. Wenn der Anbieter seine empfohlene statische Version aktualisiert, aktualisiert er AWS WAF automatisch die Standardversionseinstellung für die Regelgruppe in Ihrer Web-ACL.

Wenn Sie die Standardversion einer verwalteten Regelgruppe verwenden, führen Sie die folgenden Schritte aus (bewährte Methode):

- Benachrichtigungen abonnieren – Abonnieren Sie Benachrichtigungen für Änderungen an der Regelgruppe und behalten Sie diese im Auge. Die meisten Anbieter senden im Voraus Benachrichtigungen über neue statische Versionen und Änderungen der Standardversion. Damit können Sie die Auswirkungen einer neuen statischen Version überprüfen, bevor Sie zur Standardversion wechseln. Weitere Informationen finden Sie unter [Erhalten von Benachrichtigungen zu neuen Versionen und Aktualisierungen](#).
- Überprüfen Sie die Auswirkungen der statischen Versionseinstellungen und nehmen Sie gegebenenfalls Anpassungen vor, bevor Ihre Standardversion auf eine neue statische Version festgelegt wird. Bevor Ihre Standardversion auf eine neue statische Version festgelegt wird, überprüfen Sie die Auswirkungen der statischen Version auf die Überwachung und Verwaltung Ihrer Webanfragen. Für die neue statische Version müssen möglicherweise neue Regeln überprüft werden. Suchen Sie nach falsch positiven Ergebnissen oder anderem unerwarteten Verhalten, falls Sie die Verwendung der Regelgruppe ändern müssen. Beispielsweise können Sie Regeln zum Zählen festlegen, damit sie nicht den Datenverkehr blockieren, während Sie bestimmen, wie Sie mit dem neuen Verhalten umgehen möchten. Weitere Informationen finden Sie unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).
- Statische Version – Wenn Sie eine unveränderliche Version verwenden möchten, müssen Sie die Versionseinstellung manuell aktualisieren, sobald Sie bereit sind, auf eine neue Version der Regelgruppe umzustellen.

Wenn Sie eine statische Version einer verwalteten Regelgruppe verwenden, führen Sie die folgenden Schritte aus (bewährte Methode):

- Version immer auf dem neuesten Stand halten – Achten Sie darauf, dass Sie immer eine möglichst neue Version Ihrer verwalteten Regelgruppe verwenden. Wenn eine neue Version veröffentlicht wird, testen Sie sie, passen Sie die Einstellungen nach Bedarf an und implementieren Sie sie zeitnah. Informationen zum Testen finden Sie unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).
- Benachrichtigungen abonnieren — Abonnieren Sie Benachrichtigungen über Änderungen an der Regelgruppe, damit Sie wissen, wann Ihr Anbieter neue statische Versionen veröffentlicht. Die meisten Anbieter benachrichtigen Sie im Voraus über Versionsänderungen. Darüber hinaus muss Ihr Anbieter möglicherweise die statische Version, die Sie verwenden, aktualisieren, um eine Sicherheitslücke zu schließen oder aus anderen dringenden Gründen. Wenn Sie die Benachrichtigungen des Anbieters abonniert haben, sind Sie immer auf dem aktuellen Stand. Weitere Informationen finden Sie unter [Erhalten von Benachrichtigungen zu neuen Versionen und Aktualisierungen](#).
- Vermeiden Sie das Ablaufen von Versionen — Lassen Sie nicht zu, dass eine statische Version abläuft, während Sie sie verwenden. Die Handhabung von abgelaufenen Versionen kann je nach Anbieter variieren. Manche Anbieter erzwingen das Upgrade auf eine verfügbare Version oder andere Änderungen, die unerwartete Folgen haben können. Verfolgen Sie die AWS WAF Ablaufmetrik und stellen Sie einen Alarm ein, der Ihnen genügend Tage zur Verfügung stellt, um erfolgreich auf eine unterstützte Version zu aktualisieren. Weitere Informationen finden Sie unter [Verfolgen des Versionsablaufs](#).

Arbeiten mit verwalteten Regelgruppen

Dieser Abschnitt enthält Anleitungen für den Zugriff auf und die Verwaltung Ihrer verwalteten Regelgruppen.

Wenn Sie Ihrer Web-ACL eine verwaltete Regelgruppe hinzufügen, können Sie dieselben Konfigurationsoptionen wie für Ihre eigenen Regelgruppen sowie zusätzliche Einstellungen auswählen.

Über die Konsole greifen Sie auf Informationen zu verwalteten Regelgruppen zu, während Sie die Regeln in Ihren Web-ACLs hinzufügen und bearbeiten. Über die APIs und die Befehlszeilenschnittstelle (CLI) können Sie direkt Informationen zu verwalteten Regelgruppen anfordern.

Wenn Sie eine verwaltete Regelgruppe in Ihrer Web-ACL verwenden, können Sie die folgenden Einstellungen bearbeiten:

- Version – Diese Einstellung ist nur verfügbar, wenn die Regelgruppe versioniert ist. Weitere Informationen finden Sie unter [Versionsverwaltung mit verwalteten Regelgruppen](#).
- Regelaktionen überschreiben — Sie können die Aktionen für Regeln in der Regelgruppe durch eine beliebige Aktion außer Kraft setzen. Sie auf zu setzen, Count ist nützlich, um eine Regelgruppe zu testen, bevor Sie sie zur Verwaltung Ihrer Webanfragen verwenden. Weitere Informationen finden Sie unter [Regelaktionen überschreiben](#).
- Scope-down statement (Eingrenzungsanweisung) – Sie können eine Eingrenzungsanweisung hinzufügen, um Webanforderungen herauszufiltern, die Sie nicht mit der Regelgruppe auswerten möchten. Weitere Informationen finden Sie unter [Eingrenzungsanweisungen](#).
- Override rule group action (Aktion der Regelgruppe überschreiben) – Sie können die Aktion, die sich aus der Regelgruppenauswertung ergibt, überschreiben und auf Count festlegen. Diese Option wird nicht oft verwendet. Es ändert nichts daran, wie die Regeln in der Regelgruppe AWS WAF ausgewertet werden. Weitere Informationen finden Sie unter [Aktion der Regelgruppe überschreiben zu Count](#).

So bearbeiten Sie die Einstellungen für verwaltete Regelgruppen in Ihrer Web-ACL

- Konsole
 - (Option) Wenn Sie die verwaltete Regelgruppe zu Ihrer Web-ACL hinzufügen, können Sie Edit (Bearbeiten) wählen, um die Einstellungen anzuzeigen und zu bearbeiten.
 - (Option) Nachdem Sie die verwaltete Regelgruppe zu Ihrer Web-ACL hinzugefügt haben, wählen Sie auf der Seite Web ACLs die neu erstellte Web-ACL. Dies führt Sie zur Bearbeitungsseite der Web-ACL.
 - Wählen Sie Rules (Regeln) aus.
 - Wählen Sie die Regelgruppe aus und wählen Sie dann Edit (Bearbeiten), um die Einstellungen anzuzeigen und zu bearbeiten.
- APIs und CLI – Außerhalb der Konsole können Sie die Einstellungen von verwalteten Regelgruppen verwalten, wenn Sie die Web-ACL erstellen und aktualisieren.

Abrufen der Liste der verwalteten Regelgruppen

Sie können die Liste der verwalteten Regelgruppen abrufen, die Sie in Ihren Web-ACLs verwenden können. Die Liste umfasst Folgendes:

- Alle Regelgruppen für AWS verwaltete Regeln.
- Die AWS Marketplace Regelgruppen, die Sie abonniert haben.

Note

Informationen zum Abonnieren von AWS Marketplace Regelgruppen finden Sie unter. [AWS Marketplace verwaltete Regelgruppen](#)

Wenn Sie die Liste der verwalteten Regelgruppen abrufen, hängt der Inhalt der Liste davon ab, welche Schnittstelle Sie verwenden:

- Konsole — Über die Konsole können Sie alle verwalteten Regelgruppen sehen, einschließlich der AWS Marketplace Regelgruppen, die Sie noch nicht abonniert haben. Für die noch nicht abonnierten Regelgruppen finden Sie auf der Benutzeroberfläche Links, mit denen Sie sie abonnieren können.
- APIs und CLI – Außerhalb der Konsole werden bei Ihrer Anforderung nur die Regelgruppen zurückgegeben, die für Sie verfügbar sind.

So rufen Sie die Liste der verwalteten Regelgruppen ab

- Konsole – Wählen Sie während des Erstellungsprozesses einer Web-ACL auf der Seite Add rules and rule groups (Regeln und Regelgruppen hinzufügen) die Option Add managed rule groups (Verwaltete Regelgruppen hinzufügen). Auf der obersten Ebene werden die Anbieternamen aufgelistet. Erweitern Sie die Anbieterlisten, um die Liste der verwalteten Regelgruppen anzuzeigen. Für versionierte Regelgruppen werden auf dieser Ebene die Informationen für die Standardversion angezeigt. Wenn Sie eine verwaltete Regelgruppe zu Ihrer Web-ACL hinzufügen, listet die Konsole sie basierend auf dem Namensschema <Vendor Name>-<Managed Rule Group Name> auf.
- API –
 - ListAvailableManagedRuleGroups
- CLI –

- `aws wafv2 list-available-managed-rule-groups --scope=<CLOUDFRONT | REGIONAL>`

Abrufen der Regeln in einer verwalteten Regelgruppe

Sie können eine Liste der Regeln in einer verwalteten Regelgruppe abrufen. Die API- und CLI-Aufrufe geben die Regelspezifikationen zurück, auf die Sie im JSON-Modell oder über dieses verweisen können AWS CloudFormation.

So rufen Sie die Liste der Regeln in einer verwalteten Regelgruppe ab

- Konsole
 - (Option) Wenn Sie die verwaltete Regelgruppe zu Ihrer Web-ACL hinzufügen, können Sie Edit (Bearbeiten) wählen, um die Regeln anzuzeigen.
 - (Option) Nachdem Sie die verwaltete Regelgruppe zu Ihrer Web-ACL hinzugefügt haben, wählen Sie auf der Seite Web ACLs (Web-ACLs) die neu erstellte Web-ACL. Dies führt Sie zur Bearbeitungsseite der Web-ACL.
 - Wählen Sie Rules (Regeln) aus.
 - Wählen Sie die Regelgruppe aus, für die Sie eine Regelliste anzeigen möchten, und klicken Sie dann auf Bearbeiten. AWS WAF zeigt die Liste der Regeln in der Regelgruppe an.
- API – `DescribeManagedRuleGroup`
- CLI – `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT | REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Abrufen der verfügbaren Versionen für eine verwaltete Regelgruppe

Die verfügbaren Versionen einer verwalteten Regelgruppe sind diejenigen Versionen, deren Ablauf noch nicht geplant ist. In der Liste wird angegeben, welche Version die aktuelle Standardversion für die Regelgruppe ist.

So rufen Sie eine Liste der verfügbaren Versionen einer verwalteten Regelgruppe ab

- Konsole
 - (Option) Wenn Sie die verwaltete Regelgruppe zu Ihrer Web-ACL hinzufügen, wählen Sie Edit (Bearbeiten), um die Informationen zur Regelgruppe anzuzeigen. Erweitern Sie das Dropdownmenü Version, um die Liste der verfügbaren Versionen anzuzeigen.

- (Option) Nachdem Sie die verwaltete Regelgruppe zu Ihrer Web-ACL hinzugefügt haben, wählen Sie in der Web-ACL die Option Edit (Bearbeiten) und wählen Sie dann die Regelgruppenregel aus und bearbeiten Sie sie. Erweitern Sie das Dropdownmenü Version, um die Liste der verfügbaren Versionen anzuzeigen.
- API –
 - `ListAvailableManagedRuleGroupVersions`
- CLI –
 - `aws wafv2 list-available-managed-rule-group-versions --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Hinzufügen einer verwalteten Regelgruppe zu einer Web-ACL über die Konsole

Diese Anleitung gilt für alle Regelgruppen mit AWS verwalteten Regeln und für die AWS Marketplace Regelgruppen, die Sie abonniert haben.

Risiken rund um Produktionsdatenverkehr

Bevor Sie Änderungen in Ihrer Web-ACL für den Produktionsdatenverkehr implementieren, testen und optimieren Sie sie in einer Staging- oder Testumgebung, bis Sie mit den möglichen Auswirkungen auf Ihren Datenverkehr zufrieden sind. Testen und optimieren Sie anschließend Ihre aktualisierten Regeln im Zählmodus mit Ihrem Produktionsdatenverkehr, bevor Sie sie aktivieren. Anleitungen finden Sie unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

Note

Bei der Verwendung von mehr als 1.500 WCUs in einer Web-ACL fallen Kosten an, die über den Grundpreis für Web-ACL hinausgehen. Weitere Informationen finden Sie unter [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#) und [Preise zu AWS WAF](#).

So fügen Sie eine verwaltete Regelgruppe über die Konsole zu einer Web-ACL hinzu

1. [Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter https://console.aws.amazon.com/wafv2/.](https://console.aws.amazon.com/wafv2/)

2. Wählen Sie im Navigationsbereich Web ACLs aus.
3. Wählen Sie auf der Seite Web ACLs aus der Liste der Web-ACLs diejenige aus, der Sie die Regelgruppe hinzufügen möchten. Sie werden zur Seite der einzelnen Web-ACL weitergeleitet.
4. Wählen Sie auf der Seite der Web-ACL die Registerkarte Rules (Regeln) aus.
5. Wählen Sie im Bereich Rules (Regeln) die Option Add rules (Regeln hinzufügen) und dann die Option Add managed rule groups (Verwaltete Regelgruppen hinzufügen) aus.
6. Erweitern Sie auf der Seite Add managed rule groups (Verwaltete Regelgruppen hinzufügen) die Auswahl für Ihren Regelgruppen-Anbieter, um die Liste der verfügbaren Regelgruppen anzuzeigen.
7. Wählen Sie für jede Regelgruppe, die Sie hinzufügen möchten, die Option Add to web ACL (Zu Web-ACL hinzufügen) aus. Wenn Sie die Konfiguration der Web-ACL für die Regelgruppe ändern möchten, wählen Sie Edit (Bearbeiten), nehmen Sie die gewünschten Änderungen vor und wählen Sie dann Save rule (Regel speichern). Weitere Informationen zu den Optionen finden Sie in der Anleitung zur Versionsverwaltung unter [Versionsverwaltung mit verwalteten Regelgruppen](#) und in der Anleitung zur Verwendung einer verwalteten Regelgruppe in einer Web-ACL unter [Verwaltete Regelgruppenanweisung](#).
8. Wählen Sie unten auf der Seite Add managed rule groups (Verwaltete Regelgruppen hinzufügen) die Option Add rules (Regeln hinzufügen).
9. Passen Sie auf der Seite Set rule priority (Regelpriorität festlegen) die Reihenfolge, in der die Regeln ausgeführt werden, nach Bedarf an und wählen Sie dann Save (Speichern) aus. Weitere Informationen finden Sie unter [Reihenfolge der Verarbeitung von Regeln und Regelgruppen in einer Web-ACL](#).

Auf der Seite Ihrer Web-ACL werden die von Ihnen hinzugefügten verwalteten Regelgruppen auf der Registerkarte Regeln (Regeln) aufgelistet.

Testen und optimieren Sie alle Änderungen an Ihren AWS WAF Schutzmaßnahmen, bevor Sie sie für den Produktionsdatenverkehr verwenden. Weitere Informationen finden Sie unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

Temporäre Inkonsistenzen bei Updates

Wenn Sie eine Web-ACL oder andere AWS WAF Ressourcen erstellen oder ändern, dauert es nicht lange, bis die Änderungen in allen Bereichen, in denen die Ressourcen gespeichert sind, übernommen werden. Die Übertragungszeit kann zwischen einigen Sekunden und mehreren Minuten liegen.

Im Folgenden finden Sie Beispiele für temporäre Inkonsistenzen, die Ihnen bei der Übertragung von Änderungen möglicherweise auffallen:

- Wenn Sie nach der Erstellung einer Web-ACL versuchen, sie einer Ressource zuzuordnen, wird möglicherweise eine Ausnahme angezeigt, die darauf hinweist, dass die Web-ACL nicht verfügbar ist.
- Nachdem Sie einer Web-ACL eine Regelgruppe hinzugefügt haben, gelten die neuen Regelgruppenregeln möglicherweise in einem Bereich, in dem die Web-ACL verwendet wird, und nicht in einem anderen.
- Nachdem Sie eine Regelaktionseinstellung geändert haben, sehen Sie möglicherweise an einigen Stellen die alte Aktion und an anderen die neue Aktion.
- Nachdem Sie einem IP-Set, das in einer Sperrregel verwendet wird, eine IP-Adresse hinzugefügt haben, wird die neue Adresse möglicherweise in einem Bereich blockiert, während sie in einem anderen weiterhin zulässig ist.


Erhalten von Benachrichtigungen zu neuen Versionen und Aktualisierungen einer verwalteten Regelgruppe

Ein Anbieter verwalteter Regelgruppen verwendet SNS-Benachrichtigungen, um Regelgruppenänderungen wie bevorstehende neue Versionen und dringende Sicherheitsupdates anzukündigen.

Wie abonniere ich SNS-Benachrichtigungen

Um Benachrichtigungen für eine Regelgruppe zu abonnieren, erstellen Sie ein Amazon SNS-Abonnement für den Amazon SNS-Thema-ARN der Regelgruppe in der Region „USA Ost (Nord-Virginia)“ (us-east-1).

Weitere Informationen zum Abonnieren finden Sie im [Entwicklerhandbuch zu Amazon Simple Notification Service](#).

 Note

Erstellen Sie Ihr Abonnement für das SNS-Thema nur in der Region „us-east-1“.

Wo finde ich den Amazon SNS-Thema-ARN für eine verwaltete Regelgruppe?

AWS Regelgruppen für verwaltete Regeln verwenden einen einzigen SNS-Themen-ARN, sodass Sie den Themen-ARN aus einer der Regelgruppen abrufen und abonnieren können, um Benachrichtigungen für alle Regelgruppen mit AWS verwalteten Regeln zu erhalten, die SNS-Benachrichtigungen bereitstellen.

- Konsole
 - (Option) Wenn Sie die verwaltete Regelgruppe zu Ihrer Web-ACL hinzufügen, wählen Sie Edit (Bearbeiten), um die Informationen zur Regelgruppe anzuzeigen. Dazu zählt auch der Amazon SNS-Thema-ARN der Regelgruppe.
 - (Option) Nachdem Sie die verwaltete Regelgruppe zu Ihrer Web-ACL hinzugefügt haben, wählen Sie in der Web-ACL die Option Edit (Bearbeiten) und wählen Sie dann die Regelgruppenregel aus und bearbeiten Sie sie, um den Amazon SNS-Thema-ARN der Regelgruppe zu sehen.
- API – DescribeManagedRuleGroup
- CLI – `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT | REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Versionierung und SNS-Benachrichtigungen für AWS Regelgruppen mit verwalteten Regeln

Alle Regelgruppen mit AWS verwalteten Regeln bieten Versionsverwaltungs- und SNS-Aktualisierungsbenachrichtigungen, mit Ausnahme der Regelgruppen für IP-Reputation, Bot-Kontrolle und Verhinderung von Kontoübernahmen.

Die Regelgruppen für AWS verwaltete Regeln, die Benachrichtigungen bereitstellen, verwenden alle dasselbe SNS-Thema Amazon Resource Name (ARN).

Für Bereitstellungen, die sich auf Ihren Schutz auswirken, wie z. B. Änderungen an der Standardversion, AWS bietet es SNS-Benachrichtigungen, um Sie über geplante Bereitstellungen zu informieren und Sie darüber zu informieren, wann eine Bereitstellung beginnt. Bei Bereitstellungen, die Ihren Schutz nicht beeinträchtigen, wie z. B. Release-Candidate-Bereitstellungen und Bereitstellungen statischer Versionen, werden Sie AWS möglicherweise benachrichtigt, nachdem die Bereitstellung gestartet oder sogar abgeschlossen wurde. Nach Abschluss der Bereitstellung einer neuen statischen Version aktualisiert dieses Handbuch im Changelog unter [AWS Changelog für verwaltete Regeln](#) und auf der Seite mit dem Dokumentverlauf unter [Dokumentverlauf](#) Weitere Informationen zu den Benachrichtigungen, die für die einzelnen Bereitstellungstypen bereitgestellt werden, finden Sie unter [Bereitstellungen für versionierte Regelgruppen mit AWS verwalteten Regeln](#).

Abonnieren Sie den RSS-Feed von einer beliebigen HTML-Seite dieses Handbuchs und abonnieren Sie das SNS-Thema für die Regelgruppen mit AWS verwalteten Regeln, um alle Updates für die Regelgruppen mit AWS verwalteten Regeln zu erhalten. AWS

Die Felder in den Amazon SNS SNS-Benachrichtigungen enthalten immer den Betreff, die Nachricht und MessageAttributes. Zusätzliche Felder hängen von der Art der Nachricht und der verwalteten Regelgruppe ab, für die die Benachrichtigung bestimmt ist. Im Folgenden finden Sie ein Beispiel für eine Benachrichtigungsliste fürAWSManagedRulesCommonRuleSet.

```
{
  "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"
    }
  }
}
```

Allgemeine Informationen zu Amazon SNS-Benachrichtigungsformaten und dazu, wie Sie die eingehenden Benachrichtigungen filtern, finden Sie unter [Analysieren von Nachrichtenformaten](#) und [Filterrichtlinien für Amazon SNS-Abonnements](#) im Amazon Simple Notification Service-Entwicklerhandbuch.

Verfolgen des Versionsablaufs einer Regelgruppe

Wenn Sie eine bestimmte Version einer Regelgruppe verwenden, stellen Sie sicher, dass Sie eine Version nach ihrem Ablaufdatum nicht weiter verwenden.

Tip

Wenn Sie bevorstehende Änderungen für die verwaltete Regelgruppe über Amazon SNS verfolgen, erhalten Sie Benachrichtigungen über neue und empfohlene Versionen. Wenn Sie regelmäßig eine neuere Version testen und dann zu dieser neueren Version wechseln, sind Sie den Ablaufaktivitäten der älteren Versionen stets voraus. Sie profitieren außerdem von den aktuellsten Schutzmaßnahmen der Regelgruppe. Weitere Informationen zu Benachrichtigungen finden Sie unter [Erhalten von Benachrichtigungen zu neuen Versionen und Aktualisierungen](#).

Wenn eine Version, die Sie verwenden, abgelaufen ist, werden Änderungen an der Web-ACL AWS WAF blockiert, in der Sie die Regelgruppe verwenden. Diese Blockierung bleibt bestehen, bis Sie die Regelgruppe auf eine verfügbare Version aktualisieren oder aus Ihrer Web-ACL entfernen.

Wie eine verwaltete Regelgruppe bei einem Versionsablauf behandelt wird, hängt vom Anbieter der jeweiligen Regelgruppe ab. Bei verwalteten AWS -Regelgruppen wird die Version automatisch in die Standardversion der Regelgruppe geändert. Fragen Sie bei AWS Marketplace Regelgruppen den Anbieter, wie er mit dem Ablauf umgeht.

Um die Ablaufplanung für eine verwaltete Regelgruppe zu überwachen, verfolgen Sie die CloudWatch Ablaufmetriken von Amazon anhand von AWS WAF:

- Metrikname: DaysToExpiry
- Metrikdimensionen: Region, ManagedRuleGroup, Vendor und Version

Suchen Sie die Metrik für Ihre verwaltete Regelgruppe in Amazon CloudWatch und stellen Sie einen Alarm ein, sodass Sie rechtzeitig benachrichtigt werden, um zu einer neueren Version Ihrer Regelgruppe zu wechseln. Informationen zur Verwendung von CloudWatch Amazon-Metriken und zur Konfiguration von Alarmen finden Sie im [CloudWatch Amazon-Benutzerhandbuch](#).

Wenn der Anbieter eine neue Version der Regelgruppe erstellt, legt er auch die voraussichtliche Lebensdauer der Version fest. Es ist zwar nicht geplant, dass die Version abläuft, aber der Metrikwert

ist auf die Einstellung für die prognostizierte Lebensdauer festgelegt, und in CloudWatch wird ein pauschaler Wert für die Metrik angezeigt. Nachdem der Anbieter den Ablauf der Metrik geplant hat, nimmt der Metrikerwert jeden Tag ab, bis er am Tag des Ablaufs Null erreicht.

Wenn Sie eine verwaltete Regelgruppe in Ihrer Web-ACL haben, die den Datenverkehr auswertet, erhalten Sie eine Metrik dafür. Die Metrik ist nur für aktiv verwendete Regelgruppen verfügbar.

Beispielkonfigurationen für verwaltete Regelgruppen in JSON und YAML

Die API- und CLI-Aufrufe geben eine Liste aller Regeln in der verwalteten Regelgruppe zurück, auf die Sie im JSON-Modell oder über dieses verweisen können AWS CloudFormation.

JSON

Mit JSON können Sie verwaltete Regelgruppen innerhalb einer Regelanweisung referenzieren und ändern. Die folgende Liste zeigt die Regelgruppe „AWS Verwaltete Regeln“ im JSON-Format. `AWSManagedRulesCommonRuleSet` In der `RuleActionOverrides` Spezifikation ist eine Regel aufgeführt, deren Aktion überschrieben wurde. `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

Sie können verwaltete Regelgruppen innerhalb einer Regelanweisung mit der AWS CloudFormation -YAML-Vorlage referenzieren und ändern. Die folgende Liste zeigt die Regelgruppe „AWS Verwaltete Regeln“ in AWS CloudFormation der AWSManagedRulesCommonRuleSet Vorlage. In der RuleActionOverrides Spezifikation ist eine Regel aufgeführt, deren Aktion überschrieben wurde.

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 Verwaltete Regeln für AWS WAF

AWS Managed Rules for AWS WAF ist ein verwalteter Dienst, der Schutz vor häufigen Anwendungsschwachstellen oder anderem unerwünschten Datenverkehr bietet. Sie haben die

Möglichkeit, unter AWS Verwaltete Regeln für jede Web-ACL eine oder mehrere Regelgruppen bis zur maximalen Web-ACL-Kapazitätseinheit (WCU) auszuwählen.

Vermeidung von Fehlalarmen und Testen von Regelgruppenänderungen

Bevor Sie eine verwaltete Regelgruppe in der Produktion verwenden, testen Sie sie in einer Nicht-Produktionsumgebung gemäß den Anweisungen unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#). Folgen Sie den Anweisungen zum Testen und Optimieren, wenn Sie Ihrer Web-ACL eine Regelgruppe hinzufügen, um eine neue Version einer Regelgruppe zu testen und immer dann, wenn eine Regelgruppe Ihren Web-Traffic nicht so verarbeitet, wie Sie es benötigen.

Gemeinsame Sicherheitsaufgaben

AWS Verwaltete Regeln sollen Sie vor gängigen Internet-Bedrohungen schützen. Wenn sie gemäß der Dokumentation verwendet werden, bieten Regelgruppen mit AWS verwalteten Regeln eine weitere Sicherheitsebene für Ihre Anwendungen. Regelgruppen mit AWS verwalteten Regeln sind jedoch nicht als Ersatz für Ihre Sicherheitsaufgaben gedacht, die durch die von Ihnen ausgewählten AWS Ressourcen bestimmt werden. Anhand des [Modells der gemeinsamen Verantwortung](#) können Sie sicherstellen, dass Ihre Ressourcen ordnungsgemäß geschützt AWS sind.

AWS Liste der Regelgruppen für verwaltete Regeln

Die Informationen, die wir für die Regeln in den Regelgruppen „AWS Verwaltete Regeln“ veröffentlichen, sollen Ihnen ausreichend Informationen zur Verfügung stellen, um die Regeln zu verwenden, ohne dass böswillige Akteure die Regeln umgehen könnten. Wenn Sie mehr Informationen benötigen, als Sie in dieser Dokumentation finden, wenden Sie sich an das [AWS Support Center](#).

In diesem Abschnitt werden die neuesten Versionen der Regelgruppen für AWS verwaltete Regeln beschrieben. Diese sehen Sie in der Konsole, wenn Sie eine verwaltete Regelgruppe zu Ihrer Web-ACL hinzufügen. Über die API können Sie diese Liste zusammen mit den AWS Marketplace verwalteten Regelgruppen, die Sie abonniert haben, telefonisch `ListAvailableManagedRuleGroups` abrufen.

Note

Informationen zum Abrufen der Versionen einer Regelgruppe mit AWS verwalteten Regeln finden Sie unter [Abrufen der verfügbaren Versionen für eine verwaltete Regelgruppe](#)

Alle Regelgruppen mit AWS verwalteten Regeln unterstützen Beschriftungen, und die Regellisten in diesem Abschnitt enthalten Labelspezifikationen. Sie können die Kennzeichnungen für eine verwaltete Regelgruppe über die API abrufen, indem Sie `DescribeManagedRuleGroup` aufrufen. Die Kennzeichnungen werden in der Eigenschaft `AvailableLabels` in der Antwort aufgeführt. Weitere Informationen zur Kennzeichnung finden Sie unter [AWS WAF Labels auf Webanfragen](#).

Testen und optimieren Sie alle Änderungen an Ihren AWS WAF Schutzmaßnahmen, bevor Sie sie für den produktiven Datenverkehr verwenden. Weitere Informationen finden Sie unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

AWS Regelgruppen für verwaltete Regeln

- [Basisregelgruppen](#)
 - [Verwaltete Regelgruppe „Core Rule Set“ \(CRS\)](#)
 - [Verwaltete Regelgruppe „Admin protection“](#)
 - [Verwaltete Regelgruppe „Known Bad Inputs“](#)
- [Anwendungsfallspezifische Regelgruppen](#)
 - [Verwaltete Regelgruppe „SQL database“](#)
 - [Verwaltete Regelgruppe „Linux Operating System“](#)
 - [Verwaltete Regelgruppe „POSIX Operating System“](#)
 - [Verwaltete Regelgruppe „Windows Operating System“](#)
 - [Über PHP-Anwendung verwaltete Regelgruppe](#)
 - [WordPress Von der Anwendung verwaltete Regelgruppe](#)
- [IP-Reputationsregelgruppen](#)
 - [Amazon IP-Reputationsliste](#)
 - [Verwaltete Regelgruppe „Anonymous IP list“](#)
- [AWS WAF Regelgruppe Betrugsprävention \(ACFP\) zur Kontoerstellung bei der Betrugsbekämpfung](#)
 - [Verwenden Sie diese Regelgruppe](#)
 - [Von dieser Regelgruppe hinzugefügte Labels](#)
 - [Token-Labels](#)
 - [ACFP-Etiketten](#)
 - [Liste der Regeln zur Kontoerstellung und Betrugsprävention](#)
- [AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen \(ATP\) zur Betrugsbekämpfung](#)

- [Verwenden Sie diese Regelgruppe](#)
- [Von dieser Regelgruppe hinzugefügte Labels](#)
 - [Token-Labels](#)
 - [ATP-Etiketten](#)
- [Liste der Regeln zur Verhinderung von Kontoübernahmen](#)
- [AWS WAF Regelgruppe „Bot-Kontrolle“](#)
 - [Schutzstufen](#)
 - [Diese Regelgruppe verwenden](#)
 - [Von dieser Regelgruppe hinzugefügte Labels](#)
 - [Token-Labels](#)
 - [Beschriftungen von Bot Control](#)
 - [Liste der Bot-Control-Regeln](#)

Basisregelgruppen

Verwalte Basisregelgruppen bieten allgemeinen Schutz vor einer Vielzahl von häufigen Bedrohungen. Wählen Sie eine oder mehrere dieser Regelgruppen aus, um einen grundlegenden Schutz für Ihre Ressourcen zu gewährleisten.

Note

Die Informationen, die wir für die Regeln in den Regelgruppen „AWS Verwaltete Regeln“ veröffentlichen, sollen Ihnen ausreichend Informationen zur Verfügung stellen, damit Sie die Regeln verwenden können, ohne dass böswillige Akteure die Regeln umgehen könnten. Wenn Sie mehr Informationen benötigen, als Sie in dieser Dokumentation finden, wenden Sie sich an das [AWS Support Center](#).


Verwaltete Regelgruppe „Core Rule Set“ (CRS)

VendorName:AWS, Name:AWSManagedRulesCommonRuleSet, WCU: 700

Die Regelgruppe Core Rule Set (CRS) enthält Regeln, die allgemein für Webanwendungen gelten. Dies bietet Schutz vor der Ausnutzung einer Vielzahl von Schwachstellen, einschließlich einiger Schwachstellen mit hohem Risiko und häufig auftretender Schwachstellen, die in OWASP-

Veröffentlichungen wie [OWASP Top 10](#) beschrieben werden. Erwägen Sie, diese Regelgruppe für jeden AWS WAF Anwendungsfall zu verwenden.


Diese verwaltete Regelgruppe fügt den Webanforderungen, die sie auswertet, Labels hinzu, die für Regeln verfügbar sind, die nach dieser Regelgruppe in Ihrer Web-ACL ausgeführt werden. AWS WAF zeichnet die Labels auch anhand von CloudWatch Amazon-Metriken auf. Allgemeine Informationen zu Labels und Label-Metriken finden Sie unter [Bezeichnungen bei Webanforderungen](#) und [Kennzeichnen Sie Metriken und Dimensionen](#).

 Note

In dieser Tabelle wird die neueste statische Version dieser Regelgruppe beschrieben. Verwenden Sie für andere Versionen den API-Befehl [DescribeManagedRuleGroup](#).


Regelname	Beschreibung und Kennzeichnung
NoUserAgent_HEADER	<p>Prüft auf Anfragen, denen der User-Agent HTTP-Header fehlt.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:core-rule-set:NoUserAgent_Header</p>
UserAgent_BadBots_HEADER	<p>Prüft auf allgemeine User-Agent Header-Werte, die darauf hinweisen, dass es sich bei der Anfrage um einen böartigen Bot handelt. Beispiele für Muster sind nessus und nmap. Informationen zur Bot-Verwaltung finden Sie auch unter AWS WAF Regelgruppe „Bot-Kontrolle“.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:core-rule-set:BadBots_Header</p>

Regelname	Beschreibung und Kennzeichnung
SizeRestrictions_QUERYSTRING	<p>Prüft auf URI-Abfragezeichenfolgen, die mehr als 2.048 Byte lang sind.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:core-rule-set:SizeRestrictions_QueryString</p>
SizeRestrictions_Cookie_HEADER	<p>Prüft auf Cookie-Header, die mehr als 10.240 Byte groß sind.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:core-rule-set:SizeRestrictions_Cookie_Header</p>
SizeRestrictions_BODY	<p>Sucht nach Anforderungstexten, die größer als 8 KB (8.192 Byte) sind.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:core-rule-set:SizeRestrictions_Body</p>
SizeRestrictions_URI_PATH	<p>Prüft auf URI-Pfade, die mehr als 1.024 Byte lang sind.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:core-rule-set:SizeRestrictions_URIPath</p>

Regelname	Beschreibung und Kennzeichnung
EC2MetaDataSSRF_BODY	<p>Prüft auf Versuche, Amazon EC2-Metadaten aus dem Anfragetext herauszufiltern.</p> <div data-bbox="829 384 1507 1318" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Warning</p><p>Diese Regel überprüft den Anforderungstext nur bis zur Größenbeschränkung für die Web-ACL und den Ressourcentyp. Für Application Load Balancer und AWS AppSync ist das Limit auf 8 KB festgelegt. Für API Gateway CloudFront, Amazon Cognito, App Runner und Verified Access beträgt das Standardlimit 16 KB, und Sie können das Limit in Ihrer Web-ACL-Konfiguration auf bis zu 64 KB erhöhen. Diese Regel verwendet die Continue Option für den Umgang mit übergroßen Inhalten. Weitere Informationen finden Sie unter Umgang mit übergroßen Webanforderungskomponenten in AWS WAF.</p></div> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Body</p>


Regelname	Beschreibung und Kennzeichnung
EC2MetaDataSSRF_COOKIE	<p>Prüft auf Versuche, Amazon EC2-Metadaten aus dem Anfragecookie herauszufiltern.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Cookie</p>
EC2MetaDataSSRF_URI_PATH	<p>Prüft auf Versuche, Amazon EC2-Metadaten aus dem Pfad des Anfragen-URI herauszufiltern.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_URIPath</p>
EC2MetaDataSSRF_QUERY_ARGUMENTS	<p>Prüft auf Versuche, Amazon EC2-Metadaten aus den Anfragenabfrageargumenten herauszufiltern.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_QueryArguments</p>


Regelname	Beschreibung und Kennzeichnung
GenericLFI_QUERYARGUMENTS	<p>Prüft auf das Vorhandensein von Local File Inclusion (LFI)-Exploits in den Abfrageargumenten. Beispiele sind Pfaddurchquerungsversuche mit Techniken wie <code>../../../../</code>.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:core-rule-set:GenericLFI_QueryArguments</code></p>
GenericLFI_URI_PATH	<p>Prüft auf das Vorhandensein von Local File Inclusion (LFI)-Exploits im URI-Pfad. Beispiele sind Pfaddurchquerungsversuche mit Techniken wie <code>../../../../</code>.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:core-rule-set:GenericLFI_URIPath</code></p>


Regelname	Beschreibung und Kennzeichnung
GenericLFI_BODY	<p>Prüft auf das Vorhandensein Local File Inclusion (LFI)-Exploits im Anfragetext. Beispiele sind Pfaddurchquerungsversuche mit Techniken wie <code>../../../../</code>.</p> <div data-bbox="829 478 1508 1413" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Warning</p><p>Diese Regel überprüft den Anforderungstext nur bis zur Größenbeschränkung für die Web-ACL und den Ressourcentyp. Für Application Load Balancer und AWS AppSync ist das Limit auf 8 KB festgelegt. Für API Gateway CloudFront, Amazon Cognito, App Runner und Verified Access beträgt das Standardlimit 16 KB, und Sie können das Limit in Ihrer Web-ACL-Konfiguration auf bis zu 64 KB erhöhen. Diese Regel verwendet die Continue Option für den Umgang mit übergroßen Inhalten. Weitere Informationen finden Sie unter Umgang mit übergroßen Webanforderungskomponenten in AWS WAF.</p></div> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:core-rule-set:GenericLFI_Body</code></p>



Regelname	Beschreibung und Kennzeichnung
RestrictedExtensions_URI_PATH	<p>Prüft auf Anfragen, deren URI-Pfade Systemdateierweiterungen enthalten, deren Lesen oder Ausführen unsicher ist. Beispiele für Muster sind Erweiterungen wie <code>.log</code> und <code>.ini</code>.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:core-rule-set:RestrictedExtensions_URI_Path</code></p>
RestrictedExtensions_QUERY_ARGUMENTS	<p>Prüft auf Anfragen, deren Abfrageargumente Systemdateierweiterungen enthalten, deren Lesen oder Ausführen unsicher ist. Beispiele für Muster sind Erweiterungen wie <code>.log</code> und <code>.ini</code>.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:core-rule-set:RestrictedExtensions_QueryArguments</code></p>


Regelname	Beschreibung und Kennzeichnung
GenericRFI_QUERYARGUMENTS	<p>Prüft die Werte aller Abfrageparameter auf Versuche, RFI (Remote File Inclusion) in Webanwendungen auszunutzen, indem URLs eingebettet werden, die IPv4-Adressen enthalten. Beispiele sind Muster wie <code>http://</code>, <code>https://</code>, <code>ftp://</code>, <code>ftps://</code> und <code>file://</code> mit einem IPv4-Host-Header im Exploit-Versuch.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:core-rule-set:GenericRFI_QueryArguments</code></p>

Regelname	Beschreibung und Kennzeichnung
GenericRFI_BODY	<p>Überprüft den Anforderungstext auf Versuche, RFI (Remote File Inclusion) in Webanwendungen auszunutzen, indem URLs eingebettet werden, die IPv4-Adressen enthalten. Beispiele sind Muster wie <code>http://</code>, <code>https://</code>, <code>ftp://</code>, <code>ftps://</code> und <code>file://</code> mit einem IPv4-Host-Header im Exploit-Versuch.</p> <div data-bbox="829 621 1508 1556" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Warning</p><p>Diese Regel untersucht den Hauptteil der Anfrage nur bis zur Größenbeschränkung für die Web-ACL und den Ressourcentyp. Für Application Load Balancer und AWS AppSync ist das Limit auf 8 KB festgelegt. Für API Gateway CloudFront, Amazon Cognito, App Runner und Verified Access beträgt das Standardlimit 16 KB, und Sie können das Limit in Ihrer Web-ACL-Konfiguration auf bis zu 64 KB erhöhen. Diese Regel verwendet die Continue Option für den Umgang mit übergroßen Inhalten. Weitere Informationen finden Sie unter Umgang mit übergroßen Webanforderungskomponenten in AWS WAF.</p></div> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:core-rule-set:GenericRFI_Body</code></p>

Regelname	Beschreibung und Kennzeichnung
GenericRFI_URI_PATH	<p>Überprüft den URI-Pfad auf Versuche, RFI (Remote File Inclusion) in Webanwendungen auszunutzen, indem URLs eingebettet werden, die IPv4-Adressen enthalten. Beispiele sind Muster wie <code>http://</code>, <code>https://</code>, <code>ftp://</code>, <code>ftps://</code> und <code>file://</code> mit einem IPv4-Host-Header im Exploit-Versuch.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:core-rule-set:GenericRFI_URIPath</code></p>
CrossSiteScripting_COOKIE	<p>Überprüft mithilfe der integrierten Funktionen die Werte von Cookie-Headern auf gängige XSS-Muster (Cross-Site Scripting). AWS WAF Cross-Site-Scripting-Angriffsregel-Anweisung Beispiele für Muster sind Skripte wie <code><script>alert("hello")</script></code>.</p> <div data-bbox="829 1182 1507 1495" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Die Details zur Regelübereinstimmung in den AWS WAF Protokollen sind für Version 2.0 dieser Regelgruppe nicht aufgefüllt.</p></div> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:core-rule-set:CrossSiteScripting_Cookie</code></p>

Regelname	Beschreibung und Kennzeichnung
CrossSiteScripting_QUERYARGUMENTS	<p>Überprüft die Werte von Abfrageargumenten mithilfe der integrierten Funktion auf gängige XSS-Muster (Cross-Site Scripting). AWS WAF Cross-Site-Scripting-Angriffsregel-Anweisung Beispiele für Muster sind Skripte wie <code><script>alert("hello")</script></code> .</p> <div data-bbox="829 575 1507 888"><p> Note</p><p>Die Details zur Regelübereinstimmung in den AWS WAF Protokollen sind für Version 2.0 dieser Regelgruppe nicht aufgefüllt.</p></div> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:core-rule-set:CrossSiteScripting_QueryArguments</p>

Regelname	Beschreibung und Kennzeichnung
CrossSiteScripting_BODY	<p>Überprüft den Anforderungstext mithilfe der integrierten Funktion auf gängige XSS-Muster (Cross-Site Scripting). AWS WAF Cross-Site Scripting-Angriffsregel-Anweisung Beispiele für Muster sind Skripte wie <code><script>alert("hello")</script></code>.</p> <div data-bbox="829 575 1508 890"><p> Note</p><p>Die Details zur Regelübereinstimmung in den AWS WAF Protokollen sind für Version 2.0 dieser Regelgruppe nicht aufgefüllt.</p></div> <div data-bbox="829 989 1508 1789"><p> Warning</p><p>Diese Regel überprüft den Anforderungstext nur bis zur Größenbeschränkung für die Web-ACL und den Ressourcentyp. Für Application Load Balancer und AWS AppSync ist das Limit auf 8 KB festgelegt. Für API Gateway CloudFront, Amazon Cognito, App Runner und Verified Access beträgt das Standardlimit 16 KB, und Sie können das Limit in Ihrer Web-ACL-Konfiguration auf bis zu 64 KB erhöhen. Diese Regel verwendet die Continue Option für den Umgang mit übergroßen Inhalten. Weitere Informationen finden Sie unter Umgang mit übergroßen</p></div>

Regelname	Beschreibung und Kennzeichnung
	<p data-bbox="906 212 1474 296">Webanforderungskomponenten in AWS WAF.</p> <p data-bbox="829 436 1097 470">Regelaktion: Block</p> <p data-bbox="829 516 1442 600">Label: awswaf:managed:aws:core-rule-set:CrossSiteScripting_Body</p>
CrossSiteScripting_URIPATH	<p data-bbox="829 674 1490 951">Überprüft mithilfe der integrierten Funktionen den Wert des URI-Pfads auf gängige XSS-Muster (Cross-Site Scripting). AWS WAF Cross-Site-Scripting-Angriffsregel-Anweisung Beispiele für Muster sind Skripte wie <code><script>alert("hello")</script></code>.</p> <div data-bbox="829 993 1507 1308" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p data-bbox="862 1031 979 1064"> Note</p> <p data-bbox="906 1087 1455 1266">Die Details zur Regelübereinstimmung in den AWS WAF Protokollen sind für Version 2.0 dieser Regelgruppe nicht aufgefüllt.</p> </div> <p data-bbox="829 1409 1097 1442">Regelaktion: Block</p> <p data-bbox="829 1488 1406 1614">Label: awswaf:managed:aws:core-rule-set:CrossSiteScripting_URIPATH</p>

Verwaltete Regelgruppe „Admin protection“

VendorName:AWS, Name:AWSManagedRulesAdminProtectionRuleSet, WCU: 100

Die Regelgruppe „Admin Protection“ enthält Regeln, mit denen Sie den externen Zugriff auf offengelegte Verwaltungsseiten blockieren können. Dies kann nützlich sein, wenn Sie Software von Drittanbietern ausführen oder das Risiko verringern möchten, dass ein schädlicher Akteur administrativen Zugriff auf Ihre Anwendung erhält.

Diese verwaltete Regelgruppe fügt den Webanforderungen, die sie auswertet, Labels hinzu, die für Regeln verfügbar sind, die nach dieser Regelgruppe in Ihrer Web-ACL ausgeführt werden. AWS WAF zeichnet die Labels auch anhand von CloudWatch Amazon-Metriken auf. Allgemeine Informationen zu Labels und Label-Metriken finden Sie unter [Bezeichnungen bei Webanforderungen](#) und [Kennzeichnen Sie Metriken und Dimensionen](#).

Note

In dieser Tabelle wird die neueste statische Version dieser Regelgruppe beschrieben. Verwenden Sie für andere Versionen den API-Befehl [DescribeManagedRuleGroup](#).

Regelname	Beschreibung und Kennzeichnung
AdminProtection_URIPATH	<p>Sucht nach URI-Pfaden, die im Allgemeinen für die Verwaltung eines Webserver oder einer Anwendung reserviert sind. Ein Beispielmuster ist <code>sqlmanager</code> .</p> <p>Regelaktion: Block</p> <p>Label: <code>awswaf:managed:aws:admin-protection:AdminProtection_URIPATH</code></p>

Verwaltete Regelgruppe „Known Bad Inputs“

VendorName:AWS, Name:AWSManagedRulesKnownBadInputsRuleSet, WCU: 200


Die Regelgruppe „Known Bad Inputs“ enthält Regeln zum Blockieren von Anfragemustern, die bekanntermaßen ungültig sind und mit der Ausnutzung oder Entdeckung von Schwachstellen

verbunden sind. Dies kann dazu beitragen, das Risiko zu verringern, dass ein schädlicher Akteur eine gefährdete Anwendung entdeckt.


Diese verwaltete Regelgruppe fügt den Webanforderungen, die sie auswertet, Labels hinzu, die für Regeln verfügbar sind, die nach dieser Regelgruppe in Ihrer Web-ACL ausgeführt werden. AWS WAF zeichnet die Labels auch anhand von CloudWatch Amazon-Metriken auf. Allgemeine Informationen zu Labels und Label-Metriken finden Sie unter [Bezeichnungen bei Webanforderungen](#) und [Kennzeichnen Sie Metriken und Dimensionen](#).

Note

In dieser Tabelle wird die neueste statische Version dieser Regelgruppe beschrieben. Verwenden Sie für andere Versionen den API-Befehl [DescribeManagedRuleGroup](#).


Regelname	Beschreibung und Kennzeichnung
JavaDeserializationRCE_HEADER	<p>Untersucht die Schlüssel und Werte von HTTP-Anforderungsheadern auf Muster, die auf Versuche der Remote-Command-Ausführung (Remote Command Execution) mit Java hinweisen, wie z. B. die Sicherheitsanfälligkeiten Spring Core und Cloud Function RCE (CVE-2022-22963, CVE-2022-22965). Ein Beispielmuster ist <code>(java.lang.Runtime).getRuntime().exec("whoami")</code>.</p> <div data-bbox="829 1415 1508 1885" style="border: 1px solid #f08080; padding: 10px; margin-top: 10px;"> <p> Warning</p> <p>Diese Regel untersucht nur die ersten 8 KB der Anforderungsheader oder die ersten 200 Header, je nachdem, welcher Grenzwert zuerst erreicht wird, und verwendet die Option für die Verarbeitung übergroßer Inhalte. Continue Weitere Informationen finden Sie unter Umgang mit übergroße</p> </div>

Regelname	Beschreibung und Kennzeichnung
	<p data-bbox="906 212 1419 296">n Webanforderungskomponenten in AWS WAF.</p> <p data-bbox="829 436 1097 470">Regelaktion: Block</p> <p data-bbox="829 516 1403 646">Label: awswaf:managed:aws:known-bad-inputs:JavaDeserializatio nRCE_Header</p>


Regelname	Beschreibung und Kennzeichnung
JavaDeserializationRCE_BODY	<p>Überprüft den Anfragetext auf Muster, die auf Versuche zur Ausführung von Remote-Command-Ausführung (Remote Command Execution) mit Java hinweisen, wie z. B. die Sicherheitsanfälligkeiten Spring Core und Cloud Function RCE (CVE-2022-22963, CVE-2022-22965). Ein Beispielemuster ist <code>(java.lang.Runtime).getRuntime().exec("whoami")</code>.</p> <div data-bbox="829 716 1507 1654" style="border: 1px solid #f08080; padding: 10px;"><p> Warning</p><p>Diese Regel untersucht den Hauptteil der Anfrage nur bis zur Größenbeschränkung für den Hauptteil der Web-ACL und des Ressourcentyps. Für Application Load Balancer und AWS AppSync ist das Limit auf 8 KB festgelegt. Für API Gateway CloudFront, Amazon Cognito, App Runner und Verified Access beträgt das Standardlimit 16 KB, und Sie können das Limit in Ihrer Web-ACL-Konfiguration auf bis zu 64 KB erhöhen. Diese Regel verwendet die Continue Option für den Umgang mit übergroßen Inhalten. Weitere Informationen finden Sie unter Umgang mit übergroßen Webanforderungskomponenten in AWS WAF.</p></div> <p>Regelaktion: Block</p>

Regelname	Beschreibung und Kennzeichnung
<p>JavaDeserializationRCE_URIPATH</p>	<p>Label: awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Body</p> <p>Überprüft den Anforderungs-URI auf Muster, die auf Versuche der Java-Deserialisierung mit Remote Command Execution (Remote Command Execution) hinweisen, wie z. B. die Sicherheitslücken Spring Core und Cloud Function RCE (CVE-2022-22963, CVE-2022-22965). Ein Beispielemuster ist <code>(java.lang.Runtime).getRuntime().exec("whoami")</code>.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_URIPath</p>
<p>JavaDeserializationRCE_QUERYSTRING</p>	<p>Untersucht die Anforderungsabfragezeichenfolge auf Muster, die auf Versuche zur Deserialisierung von Java mit Remote Command Execution (RCE) hinweisen, wie z. B. die Sicherheitsanfälligkeiten Spring Core und Cloud Function RCE (CVE-2022-22963, CVE-2022-22965). Ein Beispielemuster ist <code>(java.lang.Runtime).getRuntime().exec("whoami")</code>.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_QueryString</p>

Regelname	Beschreibung und Kennzeichnung
Host_localhost_HEADER	<p>Prüft den Host-Header in der Anfrage auf Muster, die localhost anzeigen. Ein Beispielmuster ist localhost .</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:known-bad-inputs:Host_Localhost_Header</p>
PROPFIND_METHOD	<p>Prüft die HTTP-Methode in der Anfrage auf PROPFIND, eine Methode, die HEAD ähnlich ist, jedoch zusätzlich die Herausfilterung von XML-Objekten beabsichtigt.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:known-bad-inputs:Propfind_Method</p>
ExploitablePaths_URIPATH	<p>Prüft den URI-Pfad auf Versuche, auf ausnutzbare Webanwendungspfade zuzugreifen. Beispiele für Muster umfassen Pfade wie web-inf.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:known-bad-inputs:ExploitablePaths_URIPath</p>

Regelname	Beschreibung und Kennzeichnung
Log4JRCE_HEADER	<p>Überprüft die Schlüssel und Werte von Anforderungsheadern auf das Vorhandensein der Log4j-Sicherheitslücke (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) und schützt vor Versuchen mit Remote Code Execution (RCE). Ein Beispieldatum ist <code>\${jndi:ldap://example.com/}</code> .</p> <div data-bbox="829 621 1507 1222" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Warning</p><p>Diese Regel untersucht nur die ersten 8 KB der Anforderungsheader oder die ersten 200 Header, je nachdem, welcher Grenzwert zuerst erreicht wird, und verwendet die Option für die Verarbeitung übergroßer Inhalte. Weitere Informationen finden Sie unter Umgang mit übergroßen Webanforderungskomponenten in AWS WAF.</p></div> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:known-bad-inputs:Log4JRCE_Header</code></p>

Regelname	Beschreibung und Kennzeichnung
Log4JRCE_QUERYSTRING	<p><u>Überprüft die Abfragezeichenfolge auf das Vorhandensein der Log4j-Sicherheitslücke (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) und schützt vor Versuchen mit Remote Code Execution (RCE). Ein Beispielemuster ist <code>\${jndi:ldap://example.com/}</code> .</u></p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:known-bad-inputs:Log4JRCE_QueryString</p>

Regelname	Beschreibung und Kennzeichnung
Log4JRCE_BODY	<p><u>Überprüft den Text auf das Vorhandensein der Log4j-Sicherheitslücke (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) und schützt vor Versuchen mit Remote Code Execution (RCE). Ein Beispieldatum ist <code>\${jndi:ldap://example.com/}</code>.</u></p> <div data-bbox="829 575 1507 1507" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Warning</p><p>Diese Regel untersucht den Hauptteil der Anfrage nur bis zur Größenbeschränkung für den Hauptteil der Web-ACL und des Ressourcentyps. Für Application Load Balancer und AWS AppSync ist das Limit auf 8 KB festgelegt. Für API Gateway CloudFront, Amazon Cognito, App Runner und Verified Access beträgt das Standardlimit 16 KB, und Sie können das Limit in Ihrer Web-ACL-Konfiguration auf bis zu 64 KB erhöhen. Diese Regel verwendet die Continue Option für den Umgang mit übergroßen Inhalten. Weitere Informationen finden Sie unter Umgang mit übergroßen Webanforderungskomponenten in AWS WAF.</p></div> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:known-bad-inputs:Log4JRCE_Body</p>

Regelname	Beschreibung und Kennzeichnung
Log4JRCE_URIPATH	<p><u>Überprüft den URI-Pfad auf das Vorhandensein der Log4j-Sicherheitslücke (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) und schützt vor Versuchen mit Remote Code Execution (RCE). Ein Beispieldatum ist <code>\${jndi:ldap://example.com/}</code>.</u></p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:known-bad-inputs:Log4JRCE_URIPath</code></p>

Anwendungsfallsspezifische Regelgruppen

Anwendungsfallsspezifische Regelgruppen bieten inkrementellen Schutz für viele verschiedene Anwendungsfälle. AWS WAF Wählen Sie die Regelgruppen aus, die für Ihre Anwendung gelten.

Note


Die Informationen, die wir für die Regeln in den Regelgruppen „AWS Verwaltete Regeln“ veröffentlichen, sollen Ihnen genügend Informationen zur Verfügung stellen, um die Regeln zu verwenden, ohne dass böswillige Akteure die Regeln umgehen könnten. Wenn Sie mehr Informationen benötigen, als Sie in dieser Dokumentation finden, wenden Sie sich an das [AWS Support Center](#).

Verwaltete Regelgruppe „SQL database“

VendorName:AWS, Name:AWSManagedRulesSQLiRuleSet, WCU: 200


Die Regelgruppe „SQL Database“ enthält Regeln zum Blockieren von Abfragemustern, die mit der Nutzung von SQL-Datenbanken verbunden sind, z. B. SQL-Einschleusungsangriffe. Dies kann dazu beitragen, das Remote-Injection von nicht autorisierten Abfragen zu verhindern. Evaluieren Sie diese Regelgruppe, wenn Ihre Anwendung mit einer SQL-Datenbank verbunden ist.


Diese verwaltete Regelgruppe fügt den Webanforderungen, die sie auswertet, Labels hinzu, die für Regeln verfügbar sind, die nach dieser Regelgruppe in Ihrer Web-ACL ausgeführt werden. AWS WAF zeichnet die Labels auch anhand von CloudWatch Amazon-Metriken auf. Allgemeine Informationen zu Labels und Label-Metriken finden Sie unter [Bezeichnungen bei Webanforderungen](#) und [Kennzeichnen Sie Metriken und Dimensionen](#).

 Note

In dieser Tabelle wird die neueste statische Version dieser Regelgruppe beschrieben. Verwenden Sie für andere Versionen den API-Befehl [DescribeManagedRuleGroup](#).

Regelname	Beschreibung und Kennzeichnung
SQLi_QUERYARGUMENTS	<p>Verwendet die integrierte AWS WAF SQL-Injection-Angriff-Regelanweisung Funktion mit eingestellter Sensitivitätsstufe auf Low, um die Werte aller Abfrageparameter auf Muster zu überprüfen, die mit böartigem SQL-Code übereinstimmen.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:sql-database:SQLi_QueryArguments</p>
SQLiExtendedPatterns_QUERYARGUMENTS	<p>Prüft die Werte aller Abfrageparameter auf Muster, die mit böartigem SQL-Code übereinstimmen. Die Muster, nach denen diese Regel sucht, werden von der Regel SQLi_QUERYARGUMENTS nicht abgedeckt.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments</p>

Regelname	Beschreibung und Kennzeichnung
SQLi_BODY	<p>Verwendet die integrierte Funktion AWS WAF SQL-Injection-Angriff-Regelanweisung mit eingestellter Sensitivitätsstufe auf Low, um den Anfragetext auf Muster zu untersuchen, die mit böartigem SQL-Code übereinstimmen.</p> <div data-bbox="829 527 1507 1413" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Warning</p><p>Diese Regel untersucht den Anforderungstext nur bis zur Obergrenze für die Web-ACL und den Ressourcentyp. Für Application Load Balancer und AWS AppSync ist das Limit auf 8 KB festgelegt. Für API Gateway CloudFront, Amazon Cognito, App Runner und Verified Access beträgt das Standardlimit 16 KB, und Sie können das Limit in Ihrer Web-ACL-Konfiguration auf bis zu 64 KB erhöhen. Diese Regel verwendet die Continue Option für den Umgang mit übergroßen Inhalten. Weitere Informationen finden Sie unter Umgang mit übergroßen Webanforderungskomponenten in AWS WAF.</p></div> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:sql-database:SQLi_Body</p>

Regelname	Beschreibung und Kennzeichnung
SQLiExtendedPatterns_BODY	<p>Prüft den Anfragetext auf Muster, die mit böartigem SQL-Code übereinstimmen. Die Muster, nach denen diese Regel sucht, werden von der Regel nicht abgedeckt. SQLi_BODY</p> <div data-bbox="829 478 1507 1413" style="border: 1px solid #f08080; padding: 10px;"><p> Warning</p><p>Diese Regel untersucht den Hauptteil der Anfrage nur bis zur Größenbeschränkung für die Web-ACL und den Ressourcentyp. Für Application Load Balancer und AWS AppSync ist das Limit auf 8 KB festgelegt. Für API Gateway CloudFront, Amazon Cognito, App Runner und Verified Access beträgt das Standardlimit 16 KB, und Sie können das Limit in Ihrer Web-ACL-Konfiguration auf bis zu 64 KB erhöhen. Diese Regel verwendet die Continue Option für den Umgang mit übergroßen Inhalten. Weitere Informationen finden Sie unter Umgang mit übergroßen Webanforderungskomponenten in AWS WAF.</p></div> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:sql-database:SQLiExtendedPatterns_Body</p>

Regelname	Beschreibung und Kennzeichnung
SQLi_COOKIE	<p>Verwendet die integrierte Funktion AWS WAF SQL-Injection-Angriff-Regelanweisung mit eingestellter Sensitivitätsstufe auf Low, um die Header der Anforderungs-Cookies auf Muster zu untersuchen, die mit böartigem SQL-Code übereinstimmen.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:sql-data base:SQLi_Cookie</p>

Verwaltete Regelgruppe „Linux Operating System“

VendorName:AWS, Name:AWSManagedRulesLinuxRuleSet, WCU: 200

Die Regelgruppe „Linux Operating System“ enthält Regeln, die mit der Ausnutzung Linux-spezifischer Schwachstellen verbundene Anfragemuster blockieren, einschließlich Linux-spezifischer Local File Inclusion (LFI)-Angriffe. Dies kann dazu beitragen, Angriffe zu verhindern, die Dateiinhalte offenlegen oder Code ausführen, auf den der Angreifer keinen Zugriff haben soll. Sie sollten diese Regelgruppe auswerten, wenn ein Teil Ihrer Anwendung unter Linux läuft. Sie sollten diese Regelgruppe in Verbindung mit der Regelgruppe [POSIX-Betriebssystem](#) verwenden.

Diese verwaltete Regelgruppe fügt den Webanforderungen, die sie auswertet, Labels hinzu, die für Regeln verfügbar sind, die nach dieser Regelgruppe in Ihrer Web-ACL ausgeführt werden. AWS WAF zeichnet die Labels auch anhand von CloudWatch Amazon-Metriken auf. Allgemeine Informationen zu Labels und Label-Metriken finden Sie unter [Bezeichnungen bei Webanforderungen](#) und [Kennzeichnen Sie Metriken und Dimensionen](#).

Note

In dieser Tabelle wird die neueste statische Version dieser Regelgruppe beschrieben. Verwenden Sie für andere Versionen den API-Befehl [DescribeManagedRuleGroup](#).

Regelname	Beschreibung und Kennzeichnung
LFI_URIPATH	<p>Prüft den Anfragepfad auf Versuche, Local File Inclusion (LFI)-Schwachstellen in Webanwendungen auszunutzen. Beispiele für Muster umfassen Dateien wie <code>/proc/version</code>, die Angreifern Betriebssysteminformationen bereitstellen könnten.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:linux-os:LFI_URIPath</code></p>
LFI_QUERYSTRING	<p>Prüft die Werte von <code>querystring</code> auf Versuche, Local File Inclusion (LFI)-Schwachstellen in Webanwendungen auszunutzen. Beispiele für Muster umfassen Dateien wie <code>/proc/version</code>, die Angreifern Betriebssysteminformationen bereitstellen könnten.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:linux-os:LFI_QueryString</code></p>
LFI_HEADER	<p>Überprüft Anforderungsheader auf Versuche, LFI-Schwachstellen (Local File Inclusion) in Webanwendungen auszunutzen. Beispiele für Muster umfassen Dateien wie <code>/proc/version</code>, die Angreifern Betriebssysteminformationen bereitstellen könnten.</p>

Regelname	Beschreibung und Kennzeichnung
	<div data-bbox="857 247 1474 772" style="border: 1px solid #f08080; padding: 10px; background-color: #fff9e6;"> <p> Warning</p> <p>Diese Regel untersucht nur die ersten 8 KB der Anforderungsheader oder die ersten 200 Header, je nachdem, welcher Grenzwert zuerst erreicht wird, und verwendet die Option für die Behandlung übergroßer Inhalte. Continue Weitere Informationen finden Sie unter Umgang mit übergroßen Webanforderungskomponenten in AWS WAF.</p> </div> <p data-bbox="829 911 1097 947">Regelaktion: Block</p> <p data-bbox="829 993 1443 1073">Label: <code>aws:waf:managed:aws:linux-os:LFI_Header</code></p>


Verwaltete Regelgruppe „POSIX Operating System“

VendorName:AWS, Name:, WCU: AWSManagedRulesUnixRuleSet 100


Die Regelgruppe „POSIX Operating System“ enthält Regeln, die mit der Ausnutzung POSIX-spezifischer Schwachstellen und POSIX-ähnlicher Betriebssysteme verbundene Anfragemuster blockieren, einschließlich Local File Inclusion (LFI)-Angriffen. Dies kann dazu beitragen, Angriffe zu verhindern, die Dateiinhalte offenlegen oder Code ausführen, auf den der Angreifer keinen Zugriff haben soll. Sie sollten diese Regelgruppe evaluieren, wenn ein Teil Ihrer Anwendung auf einem POSIX- oder POSIX-ähnlichen Betriebssystem ausgeführt wird, wie Linux, AIX, HP-UX, macOS, Solaris, FreeBSD und OpenBSD.

Diese verwaltete Regelgruppe fügt den Webanforderungen, die sie auswertet, Labels hinzu, die für Regeln verfügbar sind, die nach dieser Regelgruppe in Ihrer Web-ACL ausgeführt werden. AWS WAF zeichnet die Labels auch anhand von CloudWatch Amazon-Metriken auf. Allgemeine

Informationen zu Labels und Label-Metriken finden Sie unter [Bezeichnungen bei Webanforderungen](#) und [Kennzeichnen Sie Metriken und Dimensionen](#).

 Note

In dieser Tabelle wird die neueste statische Version dieser Regelgruppe beschrieben. Verwenden Sie für andere Versionen den API-Befehl [DescribeManagedRuleGroup](#).

Regelname	Beschreibung und Kennzeichnung
UNIXShellCommandsVariables_QUERYARGUMENTS	<p>Prüft die Werte aller Abfrageparameter auf Versuche, Schwachstellen wie Befehlseinschleusungen, LFI und Pfaddurchquerung in Webanwendungen auszunutzen, die auf Unix-Systemen ausgeführt werden. Beispiele für Muster umfassen <code>echo \$HOME</code> und <code>echo \$PATH</code>.</p> <p>Regelaktion: Block</p> <p>Label: <code>awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QUERYARGUMENTS</code></p>
UNIXShellCommandsVariables_BODY	<p>Prüft den Anfragetext auf Versuche, Schwachstellen wie Befehlseinschleusungen, LFI und Pfaddurchquerung in Webanwendungen auszunutzen, die auf Unix-Systemen ausgeführt werden. Beispiele für Muster umfassen <code>echo \$HOME</code> und <code>echo \$PATH</code>.</p> <div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Warning</p> <p>Diese Regel überprüft den Anforderungstext nur bis zur Größenbeschränkung für die Web-ACL und den</p> </div>

Regelname	Beschreibung und Kennzeichnung
	<p>Ressourcentyp. Für Application Load Balancer und AWS AppSync ist das Limit auf 8 KB festgelegt. Für API Gateway CloudFront, Amazon Cognito, App Runner und Verified Access beträgt das Standardlimit 16 KB, und Sie können das Limit in Ihrer Web-ACL-Konfiguration auf bis zu 64 KB erhöhen. Diese Regel verwendet die Continue Option für den Umgang mit übergroßen Inhalten. Weitere Informationen finden Sie unter Umgang mit übergroßen Webanforderungskomponenten in AWS WAF.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:posix-os:UNIXShellCommandsVariables_BODY</code></p>


Verwaltete Regelgruppe „Windows Operating System“

VendorName:AWS, Name:AWSManagedRulesWindowsRuleSet, WCU: 200

Die Regelgruppe des Windows-Betriebssystems enthält Regeln, die Anforderungsmuster blockieren, die mit der Ausnutzung von Windows-spezifischen Sicherheitslücken verbunden sind, wie z. B. die Ausführung von PowerShell Befehlen aus der Ferne. Dadurch kann verhindert werden, dass Sicherheitslücken ausgenutzt werden, die es einem Angreifer ermöglichen, nicht autorisierte Befehle oder bösartigen Code auszuführen. Evaluieren Sie diese Regelgruppe, wenn ein Teil Ihrer Anwendung auf einem Windows-Betriebssystem läuft.


Diese verwaltete Regelgruppe fügt den Webanforderungen, die sie auswertet, Labels hinzu, die für Regeln verfügbar sind, die nach dieser Regelgruppe in Ihrer Web-ACL ausgeführt werden.

AWS WAF zeichnet die Labels auch anhand von CloudWatch Amazon-Metriken auf. Allgemeine Informationen zu Labels und Label-Metriken finden Sie unter [Bezeichnungen bei Webanforderungen](#) und [Kennzeichnen Sie Metriken und Dimensionen](#).


 Note

In dieser Tabelle wird die neueste statische Version dieser Regelgruppe beschrieben. Verwenden Sie für andere Versionen den API-Befehl [DescribeManagedRuleGroup](#).

Regelname	Beschreibung und Kennzeichnung
WindowsShellCommands_COOKIE	<p>Überprüft die Header der Anforderungs-Cookies auf Versuche, WindowsShell Befehle in Webanwendungen einzuschleusen. Die Übereinstimmungsmuster stellen Befehle dar <code>WindowsShell .</code> Zu den Beispielmustern gehören <code> nslookup</code> und <code>;cmd</code>.</p> <p>Regelaktion: Block</p> <p>Label: <code>awswaf:managed:aws:windows-os:WindowsShellCommands_Cookie</code></p>
WindowsShellCommands_QUERY_ARGUMENTS	<p>Prüft die Werte aller Abfrageparameter auf Versuche, WindowsShell Befehle in Webanwendungen einzuschleusen. Die Übereinstimmungsmuster stellen WindowsShell Befehle dar. Zu den Beispielmustern gehören <code> nslookup</code> und <code>;cmd</code>.</p> <p>Regelaktion: Block</p> <p>Label: <code>awswaf:managed:aws:windows-os:WindowsShellCommands_QueryArguments</code></p>

Regelname	Beschreibung und Kennzeichnung
WindowsShellCommands_BODY	<p>Überprüft den Anforderungstext auf Versuche, WindowsShell Befehle in Webanwendungen einzuschleusen. Die Übereinstimmungsmuster stellen WindowsShell Befehle dar. Zu den Beispielmustern gehören <code> nslookup</code> und <code>;cmd</code>.</p> <div data-bbox="829 575 1508 1509" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Warning</p><p>Diese Regel überprüft den Anforderungstext nur bis zur Größenbeschränkung für die Web-ACL und den Ressourcentyp. Für Application Load Balancer und AWS AppSync ist das Limit auf 8 KB festgelegt. Für API Gateway CloudFront, Amazon Cognito, App Runner und Verified Access beträgt das Standardlimit 16 KB, und Sie können das Limit in Ihrer Web-ACL-Konfiguration auf bis zu 64 KB erhöhen. Diese Regel verwendet die Continue Option für den Umgang mit übergroßen Inhalten. Weitere Informationen finden Sie unter Umgang mit übergroßen Webanforderungskomponenten in AWS WAF.</p></div> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:windows-os:WindowsShellCommands_Body</code></p>

Regelname	Beschreibung und Kennzeichnung
PowerShellCommands_COOKIE	<p>Überprüft die Header der Anforderungs-Cookies auf Versuche, PowerShell Befehle in Webanwendungen einzuschleusen. Die Übereinstimmungsmuster stellen Befehle dar PowerShell . z. B. Invoke-Expression .</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:windows-os:PowerShellCommands_Cookie</p>
PowerShellCommands_QUERYARGUMENTS	<p>Prüft die Werte aller Abfrageparameter auf Versuche, PowerShell Befehle in Webanwendungen einzuschleusen. Die Übereinstimmungsmuster stellen PowerShell Befehle dar. z. B. Invoke-Expression .</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:windows-os:PowerShellCommands_QueryArguments</p>

Regelname	Beschreibung und Kennzeichnung
PowerShellCommands_BODY	<p>Überprüft den Anforderungstext auf Versuche, PowerShell Befehle in Webanwendungen einzuschleusen. Die Übereinstimmungsmuster stellen PowerShell Befehle dar. z. B. <code>Invoke-Expression</code> .</p> <div data-bbox="829 527 1507 1461" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Warning</p><p>Diese Regel überprüft den Anforderungstext nur bis zur Größenbeschränkung für die Web-ACL und den Ressourcentyp. Für Application Load Balancer und AWS AppSync ist das Limit auf 8 KB festgelegt. Für API Gateway CloudFront, Amazon Cognito, App Runner und Verified Access beträgt das Standardlimit 16 KB, und Sie können das Limit in Ihrer Web-ACL-Konfiguration auf bis zu 64 KB erhöhen. Diese Regel verwendet die Continue Option für den Umgang mit übergroßen Inhalten. Weitere Informationen finden Sie unter Umgang mit übergroßen Webanforderungskomponenten in AWS WAF.</p></div> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:windows-os:PowerShellCommands_Body</code></p>

Über PHP-Anwendung verwaltete Regelgruppe

VendorName:AWS, Name:AWSManagedRulesPHPRuleSet, WCU: 100


Die Regelgruppe „PHP Application“ enthält Regeln, die mit der Ausnutzung von Schwachstellen im Zusammenhang mit der Programmiersprache PHP verbundene Anfragemuster blockieren, einschließlich der Einschleusung nicht sicherer PHP-Funktionen. Dadurch kann verhindert werden, dass Sicherheitslücken ausgenutzt werden, die es einem Angreifer ermöglichen, Code oder Befehle aus der Ferne auszuführen, für die er nicht autorisiert ist. Evaluieren Sie diese Regelgruppe, wenn PHP auf einem beliebigen Server installiert ist, mit dem Ihre Anwendung verbunden ist.

Diese verwaltete Regelgruppe fügt den Webanforderungen, die sie auswertet, Labels hinzu, die für Regeln verfügbar sind, die nach dieser Regelgruppe in Ihrer Web-ACL ausgeführt werden. AWS WAF zeichnet die Labels auch anhand von CloudWatch Amazon-Metriken auf. Allgemeine Informationen zu Labels und Label-Metriken finden Sie unter [Bezeichnungen bei Webanforderungen](#) und [Kennzeichnen Sie Metriken und Dimensionen](#).

Note


In dieser Tabelle wird die neueste statische Version dieser Regelgruppe beschrieben. Verwenden Sie für andere Versionen den API-Befehl [DescribeManagedRuleGroup](#).

Regelname	Beschreibung und Kennzeichnung
PHPHighRiskMethodsVariables_HEADER	Überprüft alle Header auf Versuche, PHP-Skriptcode einzuschleusen. Beispiele für Muster umfassen Funktionen wie <code>fsockopen</code> und die superglobale Variable <code>\$_GET</code> .

 **Warning**

Diese Regel untersucht nur die ersten 8 KB der Anforderungsheader oder die ersten 200 Header, je nachdem, welcher Grenzwert zuerst erreicht wird, und verwendet die Option für die Continue Behandlung übergroßer

Regelname	Beschreibung und Kennzeichnung
	<p>Inhalte. Weitere Informationen finden Sie unter Umgang mit übergroßen Webanforderungskomponenten in AWS WAF.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:php-app:PHPHighRiskMethodsVariables_Header</code></p>
PHPHighRiskMethodsVariables_QueryString	<p>Prüft alles, was ? in der Anfrage-URL nach dem ersten Wort steht, und sucht nach Versuchen, PHP-Skriptcode einzuschleusen. Beispiele für Muster umfassen Funktionen wie <code>fsockopen</code> und die superglobale Variable <code>\$_GET</code>.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:php-app:PHPHighRiskMethodsVariables_QueryString</code></p>

Regelname	Beschreibung und Kennzeichnung
PHPHighRiskMethodsVariables_BODY	<p>Prüft die Werte des Anfragetexts auf Versuche, PHP-Skriptcode einzuschleusen. Beispiele für Muster umfassen Funktionen wie <code>fsockopen</code> und die superglobale Variable <code>\$_GET</code>.</p> <div data-bbox="829 478 1507 1413" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Warning</p><p>Diese Regel überprüft den Hauptteil der Anfrage nur bis zur Größenbeschränkung für die Web-ACL und den Ressourcentyp. Für Application Load Balancer und AWS AppSync ist das Limit auf 8 KB festgelegt. Für API Gateway CloudFront, Amazon Cognito, App Runner und Verified Access beträgt das Standardlimit 16 KB, und Sie können das Limit in Ihrer Web-ACL-Konfiguration auf bis zu 64 KB erhöhen. Diese Regel verwendet die <code>Continue</code> Option für den Umgang mit übergroßen Inhalten. Weitere Informationen finden Sie unter Umgang mit übergroßen Webanforderungskomponenten in AWS WAF.</p></div> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:php-app:PHPHighRiskMethodsVariables_Body</code></p>

WordPress Von der Anwendung verwaltete Regelgruppe

VendorName:AWS, Name:AWSManagedRulesWordPressRuleSet, WCU: 100

Die Regelgruppe für WordPress Anwendungen enthält Regeln, die Anforderungsmuster blockieren, die mit der Ausnutzung von Sicherheitslücken verbunden sind, die für WordPress Websites spezifisch sind. Sie sollten diese Regelgruppe auswerten, wenn Sie sie ausführen WordPress. Diese Regelgruppe sollte in Verbindung mit den Regelgruppen [PHP-Anwendung](#) und [SQL-Datenbank](#) verwendet werden.

Diese verwaltete Regelgruppe fügt den Webanforderungen, die sie auswertet, Labels hinzu, die für Regeln verfügbar sind, die nach dieser Regelgruppe in Ihrer Web-ACL ausgeführt werden. AWS WAF zeichnet die Labels auch anhand von CloudWatch Amazon-Metriken auf. Allgemeine Informationen zu Labels und Label-Metriken finden Sie unter [Bezeichnungen bei Webanforderungen](#) und [Kennzeichnen Sie Metriken und Dimensionen](#).

Note

In dieser Tabelle wird die neueste statische Version dieser Regelgruppe beschrieben. Verwenden Sie für andere Versionen den API-Befehl [DescribeManagedRuleGroup](#).

Regelname	Beschreibung und Kennzeichnung
WordPressExploitableCommands_QUERYSTRING	<p>Überprüft die Anforderungsabfragezeichenfolge auf WordPress Befehle mit hohem Risiko, die in anfälligen Installationen oder Plugins ausgenutzt werden können. Beispiele für Muster sind Befehle wie <code>do-reset-wordpress</code> .</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:wordpress-app:WordPressExploitableCommands_QUERYSTRING</code></p>

Regelname	Beschreibung und Kennzeichnung
WordPressExploitablePaths_URI_PATH	<p>Überprüft den URI-Pfad der Anfrage auf WordPress Dateien wie <code>xmlrpc.php</code>, von denen bekannt ist, dass sie leicht ausnutzbare Sicherheitslücken aufweisen.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:wordpress-app:WordPressExploitablePaths_URI_PATH</code></p>

IP-Reputationsregelgruppen

IP-Reputationsregelgruppen blockieren Anfragen auf der Grundlage ihrer Quell-IP-Adresse.

Note

Diese Regeln verwenden die Quell-IP-Adresse aus dem Ursprung der Webanfrage. Wenn Ihr Datenverkehr über einen oder mehrere Proxys oder Load Balancer läuft, enthält der Ursprung der Webanfrage die Adresse des letzten Proxys und nicht die ursprüngliche Adresse des Clients.

Wählen Sie eine oder mehrere dieser Regelgruppen aus, wenn Sie die Gefährdung durch Bot-Datenverkehr oder Exploits reduzieren oder geografische Einschränkungen für Ihre Inhalte durchsetzen möchten. Informationen zur Bot-Verwaltung finden Sie auch unter [AWS WAF Regelgruppe „Bot-Kontrolle“](#).

Die Regelgruppen in dieser Kategorie bieten keine Versionsverwaltungs- oder SNS-Aktualisierungsbenachrichtigungen.

Note

Die Informationen, die wir für die Regeln in den Regelgruppen „AWS Verwaltete Regeln“ veröffentlichen, sollen Ihnen genügend Informationen zur Verfügung stellen, um die Regeln zu verwenden, ohne dass sie Informationen enthalten, mit denen böswillige Akteure die

Regeln umgehen könnten. Wenn Sie mehr Informationen benötigen, als Sie in dieser Dokumentation finden, wenden Sie sich an das [AWS Support Center](#).

Amazon IP-Reputationsliste

VendorName:AWS, Name:AWSManagedRulesAmazonIpReputationList, WCU: 25

Die Regelgruppe „Amazon IP Reputation List“ enthält Regeln, die auf interner Threat Intelligence von Amazon basieren. Dies ist hilfreich, wenn Sie IP-Adressen blockieren möchten, die typischerweise mit Bots oder anderen Bedrohungen verbunden sind. Das Blockieren dieser IP-Adressen kann dazu beitragen, Bots zu minimieren und das Risiko zu verringern, dass ein schädlicher Akteur eine gefährdete Anwendung entdeckt.

Diese verwaltete Regelgruppe fügt den Webanforderungen, die sie auswertet, Labels hinzu, die für Regeln verfügbar sind, die nach dieser Regelgruppe in Ihrer Web-ACL ausgeführt werden. AWS WAF zeichnet die Labels auch anhand von CloudWatch Amazon-Metriken auf. Allgemeine Informationen zu Labels und Label-Metriken finden Sie unter [Bezeichnungen bei Webanforderungen](#) und [Kennzeichnen Sie Metriken und Dimensionen](#).

Regelname	Beschreibung und Kennzeichnung
AWSManagedIPReputationList	<p>Sucht nach IP-Adressen, bei denen festgestellt wurde, dass sie aktiv an böswilligen Aktivitäten beteiligt sind. AWS WAF sammelt die IP-Adressliste aus verschiedenen Quellen, einschließlich eines Threat Intelligence-Tools MadPot, das Amazon verwendet, um Kunden vor Cyberkriminalität zu schützen. Weitere Informationen zu finden Sie MadPot unter https://www.aboutamazon.com/news/aws/amazon-madpot-stops-cybersecurity-crime.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:amazon-ip-list:AWSManagedIPReputationList</p>

Regelname	Beschreibung und Kennzeichnung
AWSManagedReconnaissanceList	<p>Sucht nach Verbindungen von IP-Adressen, die Ressourcen ausfindig machen. AWS</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:amazon-ip-list:AWSManagedReconnaissanceList</p>
AWSManagedIPDDoSList	<p>Sucht nach IP-Adressen, bei denen festgestellt wurde, dass sie aktiv an DDoS-Aktivitäten beteiligt sind.</p> <p>Regelaktion: Count</p> <p>Label: awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList</p>

Verwaltete Regelgruppe „Anonymous IP list“

VendorName:AWS, Name:AWSManagedRulesAnonymousIpList, WCU: 50

Die Regelgruppe „Liste anonymer IP-Adressen“ enthält Regeln zum Blockieren von Anfragen von Diensten, die die Verschleierung der Identität des Betrachters ermöglichen. Dazu gehören Anfragen von VPNs, Proxys, Tor-Knoten und Webhosting-Anbietern. Diese Regelgruppe ist nützlich, wenn Sie Betrachter herausfiltern möchten, die möglicherweise versuchen, ihre Identität vor Ihrer Anwendung zu verbergen. Das Blockieren der IP-Adressen dieser Services kann dazu beitragen, Bots und Möglichkeiten zur Umgehung geografischer Einschränkungen zu minimieren.

Diese verwaltete Regelgruppe fügt den Webanfragen, die sie auswertet, Labels hinzu, die für Regeln verfügbar sind, die nach dieser Regelgruppe in Ihrer Web-ACL ausgeführt werden. AWS WAF zeichnet die Labels auch anhand von CloudWatch Amazon-Metriken auf. Allgemeine Informationen zu Labels und Label-Metriken finden Sie unter [Bezeichnungen bei Webanforderungen](#) und [Kennzeichnen Sie Metriken und Dimensionen](#).

Regelname	Beschreibung und Kennzeichnung
AnonymousIPList	<p>Prüft auf eine Liste von IP-Adressen von Quellen, die Clientinformationen anonymisieren, wie Tor-Knoten, temporäre Proxys und andere Maskierungsdienste.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:anonymous-ip-list:AnonymousIPList</code></p>
HostingProviderIPList	<p>Sucht nach einer Liste mit IP-Adressen von Webhosting- und Cloud-Anbietern, von denen die Wahrscheinlichkeit geringer ist, dass sie Endbenutzer-Traffic generieren. Die IP-Liste enthält keine AWS IP-Adressen.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:anonymous-ip-list:HostingProviderIPList</code></p>

AWS WAF Regelgruppe Betrugsprävention (ACFP) zur Kontoerstellung bei der Betrugsbekämpfung

VendorName:AWS, Name:AWSManagedRulesACFPRuleSet, WCU: 50


Die AWS WAF verwaltete Regelgruppe Fraud Control Account Creation Fraud Prevention (ACFP) kennzeichnet und verwaltet Anfragen, die Teil betrügerischer Kontoerstellungsversuche sein könnten. Zu diesem Zweck überprüft die Regelgruppe Anfragen zur Kontoerstellung, die Kunden an die Registrierungs- und Kontoerstellungsendpunkte Ihrer Anwendung senden.

Die ACFP-Regelgruppe überprüft Versuche zur Kontoerstellung auf verschiedene Weise, um Ihnen Transparenz und Kontrolle über potenziell bösartige Interaktionen zu geben. Die Regelgruppe verwendet Anforderungstoken, um Informationen über den Client-Browser und den Grad der menschlichen Interaktivität bei der Erstellung der Anfrage zur Kontoerstellung zu sammeln. Die Regelgruppe erkennt und verwaltet Versuche zur Erstellung mehrerer Konten, indem sie Anfragen nach IP-Adresse und Clientsitzung aggregiert und anhand der bereitgestellten Kontoinformationen

wie der physischen Adresse und Telefonnummer aggregiert. Darüber hinaus erkennt und blockiert die Regelgruppe die Erstellung neuer Konten unter Verwendung kompromittierter Anmeldeinformationen. Dies trägt zum Schutz der Sicherheitslage Ihrer Anwendung und Ihrer neuen Benutzer bei.

Verwenden Sie diese Regelgruppe

Diese Regelgruppe erfordert eine benutzerdefinierte Konfiguration, die die Angabe der Kontoregistrierungs- und Kontoerstellungspfade Ihrer Anwendung umfasst. Sofern nicht anders angegeben, überprüfen die Regeln in dieser Regelgruppe alle Anfragen, die Ihre Clients an diese beiden Endpunkte senden. Anleitungen zur Konfiguration und Implementierung dieser Regelgruppe finden Sie unter [AWS WAF Einrichtung von Konten bei der Betrugsbekämpfung und Betrugsprävention \(ACFP\)](#).

 Note

Ihnen werden zusätzliche Gebühren berechnet, wenn Sie diese verwaltete Regelgruppe verwenden. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).

Diese Regelgruppe ist Teil der intelligenten Schutzmaßnahmen zur Abwehr von Bedrohungen in AWS WAF. Weitere Informationen finden Sie unter [AWS WAF intelligente Bedrohungsabwehr](#).

Um Ihre Kosten niedrig zu halten und sicherzustellen, dass Sie Ihren Web-Traffic nach Ihren Wünschen verwalten, verwenden Sie diese Regelgruppe gemäß den Anweisungen unter [Bewährte Methoden für intelligente Bedrohungsabwehr](#).

Diese Regelgruppe ist nicht für die Verwendung mit Amazon Cognito Cognito-Benutzerpools verfügbar. Sie können eine Web-ACL, die diese Regelgruppe verwendet, keinem Benutzerpool zuordnen, und Sie können diese Regelgruppe nicht zu einer Web-ACL hinzufügen, die bereits einem Benutzerpool zugeordnet ist.

Diese Regelgruppe bietet keine Versionsverwaltungs- oder SNS-Aktualisierungsbenachrichtigungen.

Von dieser Regelgruppe hinzugefügte Labels

Diese verwaltete Regelgruppe fügt den Webanforderungen, die sie auswertet, Labels hinzu, die für Regeln verfügbar sind, die nach dieser Regelgruppe in Ihrer Web-ACL ausgeführt werden. AWS WAF zeichnet die Labels auch anhand von CloudWatch Amazon-Metriken auf. Allgemeine Informationen zu Labels und Label-Metriken finden Sie unter [Bezeichnungen bei Webanforderungen](#) und [Kennzeichnen Sie Metriken und Dimensionen](#).

Token-Labels

Diese Regelgruppe verwendet AWS WAF Tokenverwaltung, um Webanfragen anhand des Status ihrer AWS WAF Token zu überprüfen und zu kennzeichnen. AWS WAF verwendet Token für die Nachverfolgung und Überprüfung von Clientsitzungen.

Hinweise zu Token und Tokenverwaltung finden Sie unter [AWS WAF Webanforderungstoken](#).

Informationen zu den hier beschriebenen Label-Komponenten finden Sie unter [Bezeichnungssyntax- und Benennungsanforderungen](#).

Bezeichnung der Clientsitzung

Das Label `aws:waf:managed:token:id:identifizier` enthält eine eindeutige Kennung, anhand derer die AWS WAF Tokenverwaltung die Clientsitzung identifiziert. Die Kennung kann sich ändern, wenn der Client ein neues Token erwirbt, beispielsweise nachdem er das Token, das er verwendet hat, verworfen hat.

Note

AWS WAF meldet keine CloudWatch Amazon-Metriken für dieses Label.

Token-Statusbezeichnungen: Namespace-Präfixe für Labels

Token-Statusbezeichnungen geben Auskunft über den Status des Tokens und der darin enthaltenen Challenge- und CAPTCHA-Informationen.

Jedes Token-Statuslabel beginnt mit einem der folgenden Namespace-Präfixe:

- `aws:waf:managed:token:—` Wird verwendet, um den allgemeinen Status des Tokens und den Status der Challenge-Informationen des Tokens zu melden.
- `aws:waf:managed:captcha:—` Wird verwendet, um über den Status der CAPTCHA-Informationen des Tokens zu berichten.

Token-Statusbezeichnungen: Labelnamen

Nach dem Präfix enthält der Rest des Labels detaillierte Informationen zum Token-Status:

- `accepted`— Das Anforderungstoken ist vorhanden und enthält Folgendes:

- Eine gültige Challenge oder CAPTCHA-Lösung.
- Eine noch nicht abgelaufene Herausforderung oder ein CAPTCHA-Zeitstempel.
- Eine Domainspezifikation, die für die Web-ACL gültig ist.

Beispiel: Das Label `aws-waf:managed:token:accepted` gibt an, dass das Token der Webanfragen eine gültige Challenge-Lösung, einen noch nicht abgelaufenen Challenge-Zeitstempel und eine gültige Domain enthält.

- `rejected`— Das Anforderungstoken ist vorhanden, erfüllt aber nicht die Akzeptanzkriterien.

Zusammen mit dem abgelehnten Label fügt die Tokenverwaltung einen benutzerdefinierten Label-Namespace und einen Namen hinzu, um den Grund anzugeben.

- `rejected:not_solved`— Dem Token fehlt die Challenge- oder CAPTCHA-Lösung.
- `rejected:expired`— Der Challenge- oder CAPTCHA-Zeitstempel des Tokens ist gemäß den von Ihrer Web-ACL konfigurierten Token-Immunitätszeiten abgelaufen.
- `rejected:domain_mismatch`— Die Domain des Tokens entspricht nicht der Token-Domain-Konfiguration Ihrer Web-ACL.
- `rejected:invalid`— Das angegebene Token AWS WAF konnte nicht gelesen werden.

Beispiel: Die Labels `aws-waf:managed:captcha:rejected` und `aws-waf:managed:captcha:rejected:expired` geben an, dass die Anfrage abgelehnt wurde, weil der CAPTCHA-Zeitstempel im Token die in der Web-ACL konfigurierte CAPTCHA-Token-Immunitätszeit überschritten hat.

- `absent`— Die Anfrage hat das Token nicht oder der Token-Manager konnte es nicht lesen.

Beispiel: Das Label `aws-waf:managed:captcha:absent` gibt an, dass die Anfrage das Token nicht enthält.

ACFP-Etiketten

Diese Regelgruppe generiert Beschriftungen mit dem Namespace-Präfix, `aws-waf:managed:aws:acfp:` gefolgt vom benutzerdefinierten Namespace und dem Labelnamen. Die Regelgruppe kann einer Anfrage mehr als ein Label hinzufügen.

Sie können alle Labels für eine Regelgruppe über die API abrufen, indem Sie `describeManagedRuleGroup` aufrufen. Die Kennzeichnungen werden in der Eigenschaft `AvailableLabels` in der Antwort aufgeführt.

Liste der Regeln zur Kontoerstellung und Betrugsprävention

In diesem Abschnitt sind die ACFP-Regeln `AWSMANAGEDRULESACFPRULESET` und die Bezeichnungen aufgeführt, die die Regeln der Regelgruppe Webanfragen hinzufügen.

Note

Die Informationen, die wir für die Regeln in den Regelgruppen „AWS Verwaltete Regeln“ veröffentlichen, sollen Ihnen genügend Informationen zur Verfügung stellen, um die Regeln zu verwenden, ohne dass böswillige Akteure die Regeln umgehen könnten. Wenn Sie mehr Informationen benötigen, als Sie in dieser Dokumentation finden, wenden Sie sich an das [AWS Support Center](#).


Für alle Regeln in dieser Regelgruppe ist ein Webanforderungstoken erforderlich, mit Ausnahme der ersten beiden `UnsupportedCognitoIDP` und `AllRequests`. Eine Beschreibung der Informationen, die das Token bereitstellt, finden Sie unter [Token-Eigenschaften](#).


Sofern nicht anders angegeben, überprüfen die Regeln in dieser Regelgruppe alle Anfragen, die Ihre Kunden an die Pfade zur Kontoregistrierung und Kontoerstellung senden, die Sie in der Regelgruppenkonfiguration angeben. Informationen zur Konfiguration dieser Regelgruppe finden Sie unter [AWS WAF Einrichtung von Konten bei der Betrugsbekämpfung und Betrugsprävention \(ACFP\)](#).

Regelname	Beschreibung und Kennzeichnung
<code>UnsupportedCognitoIDP</code>	<p>Prüft, ob Web-Traffic an einen Amazon Cognito Cognito-Benutzerpool gesendet wird. ACFP ist nicht für die Verwendung mit Amazon Cognito Cognito-Benutzerpools verfügbar, und diese Regel trägt dazu bei, dass die anderen ACFP-Regelgruppenregeln nicht zur Auswertung des Benutzerpool-Traffics verwendet werden.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:acfp:unsupported:cognito_idp</code></p>


Regelname	Beschreibung und Kennzeichnung
AllRequests	<p>Wendet die Regelaktion auf Anfragen an, die auf den Pfad der Registrierungsseite zugreifen . Sie konfigurieren den Pfad der Registrierungsseite, wenn Sie die Regelgruppe konfigurieren.</p> <p>Standardmäßig gilt diese Regel für Challenge Anfragen. Durch die Anwendung dieser Aktion stellt die Regel sicher, dass der Client ein Challenge-Token erhält, bevor Anfragen von den übrigen Regeln in der Regelgruppe ausgewertet werden.</p> <p>Stellen Sie sicher, dass Ihre Endbenutzer den Pfad der Registrierungsseite laden, bevor sie eine Anfrage zur Kontoerstellung einreichen.</p> <p>Token werden zu Anfragen durch die SDKs für die Client-Anwendungsintegration und durch die Regelaktionen CAPTCHA und Challenge hinzugefügt. Für eine möglichst effiziente Token-Akquisition empfehlen wir dringend, die Anwendungsintegrations-SDKs zu verwenden . Weitere Informationen finden Sie unter AWS WAF Integration von Client-Anwendungen.</p> <p>Regelaktion: Challenge</p> <p>Bezeichnung: Keine</p>


Regelname	Beschreibung und Kennzeichnung
RiskScoreHigh	<p>Prüft auf Anfragen zur Kontoerstellung mit IP-Adressen oder anderen Faktoren, die als äußerst verdächtig angesehen werden. Diese Bewertung basiert in der Regel auf mehreren Faktoren, die dazu beitragen. Sie können den <code>risk_score</code> Bezeichnungen entnehmen, die die Regelgruppe der Anfrage hinzufügt.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:acfp:risk_score:high</code></p> <p>Die Regel kann auch Labels <code>medium</code> oder <code>low</code> Risikoeinstufungen auf die Anfrage anwenden.</p> <p>Wenn die Bewertung der Risikobewertung für die Webanfrage AWS WAF nicht erfolgreich ist, fügt die Regel die Bezeichnung hinzu <code>aws:waf:managed:aws:acfp:risk_score:evaluation_failed</code></p> <p>Darüber hinaus fügt die Regel dem Namespace <code>aws:waf:managed:aws:acfp:risk_score:contributor:</code> Labels hinzu, die den Status der Risikobewertung und Ergebnisse für bestimmte Faktoren, die zur Risikobewertung beitragen, enthalten, z. B. Bewertungen der IP-Reputation und der Bewertung gestohlener Anmeldeinformationen.</p>


Regelname	Beschreibung und Kennzeichnung
SignalCredentialCompromised	<p>Durchsucht die Datenbank mit gestohlenen Anmeldeinformationen nach den Anmeldeinformationen, die in der Anfrage zur Kontoerstellung übermittelt wurden.</p> <p>Diese Regel stellt sicher, dass neue Kunden ihre Konten mit einer positiven Sicherheitslage initialisieren.</p> <div data-bbox="829 653 1507 1157" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px;"><p> Note</p><p>Sie können eine benutzerdefinierte Blockierungsantwort hinzufügen, um Ihrem Endbenutzer das Problem zu beschreiben und ihm mitzuteilen, wie er vorgehen soll. Weitere Informationen finden Sie unter ACFP-Beispiel: Benutzerdefinierte Antwort auf kompromittierte Anmeldeinformationen.</p></div> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:acfp:signal:credential_compromised</code></p> <p>Die Regelgruppe wendet das folgende zugehörige Label an, unternimmt jedoch keine Maßnahmen, da nicht alle Anfragen bei der Kontoerstellung über Anmeldeinformationen verfügen: <code>aws:waf:managed:aws:acfp:signal:missing_credential</code></p>

Regelname	Beschreibung und Kennzeichnung
SignalClientInteractivityAssessmentLow	<p>Überprüft das Token der Anfrage zur Kontoerstellung auf Daten, die auf eine abnormale menschliche Interaktion mit der Anwendung hinweisen. Menschliche Interaktivität wird anhand von Interaktionen wie Mausbewegungen und Tastendrücken erkannt. Wenn die Seite über ein HTML-Formular verfügt, umfasst die menschliche Interaktivität Interaktionen mit dem Formular.</p> <div data-bbox="829 716 1507 1360" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Diese Regel prüft nur Anfragen an den Pfad zur Kontoerstellung und wird nur ausgewertet, wenn Sie die Anwendung integrations-SDKs implementiert haben. Die SDK-Implementierungen erfassen passiv menschliche Interaktivität und speichern die Informationen im Anforderungstoken. Weitere Informationen finden Sie unter Token-Eigenschaften und AWS WAF Integration von Client-Anwendungen.</p></div> <p>Regelaktion: CAPTCHA</p> <p>Bezeichnung: Keine. Die Regel bestimmt eine Übereinstimmung auf der Grundlage verschiedener Faktoren, sodass es keine individuelle Bezeichnung gibt, die für jedes mögliche Übereinstimmungsszenario gilt.</p>


Regelname	Beschreibung und Kennzeichnung
	<p>Die Regelgruppe kann eine oder mehrere der folgenden Bezeichnungen auf Anfragen anwenden:</p> <pre>aws:waf:managed:aws:acfp:signal:client:human_interactivity:low/medium/high</pre> <pre>aws:waf:managed:aws:acfp:signal:client:human_interactivity:insufficient_data</pre> <pre>aws:waf:managed:aws:acfp:signal:form_detected</pre>
SignalAutomatedBrowser	<p>Prüft die Anfrage auf Hinweise darauf, dass der Client-Browser möglicherweise automatisiert ist.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:acfp:signal:automated_browser</code></p>
SignalBrowserInconsistency	<p>Überprüft das Token der Anfrage auf inkonsistente Browser-Abfragedaten. Weitere Informationen finden Sie unter Token-Eigenschaften.</p> <p>Regelaktion: CAPTCHA</p> <p>Label: <code>aws:waf:managed:aws:acfp:signal:browser_inconsistency</code></p>


Regelname	Beschreibung und Kennzeichnung
VolumetricIpHigh	<p>Prüft auf große Mengen von Anfragen zur Kontoerstellung, die von einzelnen IP-Adressen gesendet werden. Ein hohes Volumen besteht aus mehr als 20 Anfragen innerhalb eines Zeitfensters von 10 Minuten.</p> <div data-bbox="829 527 1507 936" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Die Schwellenwerte, für die diese Regel gilt, können aufgrund der Latenz leicht variieren. Bei einem hohen Volumen können einige Anfragen das Limit überschreiten, bevor die Regelaktion angewendet wird.</p></div> <p>Regelaktion: CAPTCHA</p> <p>Label: <code>aws:waf:managed:aws:acfp:aggregate:volumetric:ip:creation:high</code></p> <p>Die Regel wendet die folgenden Bezeichnungen auf Anfragen mit mittlerem Volumen (16-20 Anfragen pro 10-Minuten-Fenster) und geringem Volumen (11-15 Anfragen pro 10-Minuten-Fenster) an, ergreift jedoch keine Maßnahmen für sie: <code>aws:waf:managed:aws:acfp:aggregate:volumetric:ip:creation:medium</code> und <code>aws:waf:managed:aws:acfp:aggregate:volumetric:ip:creation:low</code></p>


Regelname	Beschreibung und Kennzeichnung
VolumetricSessionHigh	<p>Prüft auf große Mengen von Anfragen zur Kontoerstellung, die aus einzelnen Kundensitzungen gesendet wurden. Bei einem hohen Volumen handelt es sich um mehr als 10 Anfragen innerhalb eines Zeitfensters von 30 Minuten.</p> <div data-bbox="829 573 1507 982" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Die Schwellenwerte, für die diese Regel gilt, können aufgrund der Latenz leicht variieren. Bei einigen Anfragen wird möglicherweise das Limit überschritten, bevor die Regelaktion angewendet wird.</p></div> <p>Regelaktion: Block</p> <p>Label: <code>awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:high</code></p> <p>Die Regelgruppe wendet die folgenden Bezeichnungen auf Anfragen mit mittlerem Volumen (6-10 Anfragen pro 30-Minuten-Fenster) und geringem Volumen (2-5 Anfragen pro 30-Minuten-Fenster) an, ergreift jedoch keine Maßnahmen dafür: <code>awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:medium</code> und <code>awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:low</code></p>

Regelname	Beschreibung und Kennzeichnung
AttributeUsernameTraversalHigh	<p>Prüft auf eine hohe Anzahl von Anfragen zur Kontoerstellung aus einer einzelnen Clientsitzung, die unterschiedliche Benutzernamen verwenden. Der Schwellenwert für eine hohe Bewertung liegt bei mehr als 10 Anfragen innerhalb von 30 Minuten.</p> <div data-bbox="829 573 1507 982" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Die Schwellenwerte, für die diese Regel gilt, können aufgrund der Latenz leicht variieren. Bei einigen Anfragen wird möglicherweise das Limit überschritten, bevor die Regelaktion angewendet wird.</p></div> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:high</code></p> <p>Die Regelgruppe wendet die folgenden Bezeichnungen auf Anfragen mit mittlerem Volumen (6—10 Anfragen pro 30-Minuten-Fenster) und geringem Volumen (2—5 Anfragen pro 30-Minuten-Fenster) an, ergreift jedoch keine Maßnahmen dafür: und. <code>aws:waf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:medium</code> <code>aws:waf:managed:aws:acfp:agg</code></p>



Regelname	Beschreibung und Kennzeichnung
	<code>regate:attribute:username_t</code> <code>raversal:creation:low</code>

Regelname	Beschreibung und Kennzeichnung
VolumetricPhoneNumberHigh	<p>Prüft auf große Mengen von Anfragen zur Kontoerstellung, für die dieselbe Telefonnummer verwendet wird. Der Schwellenwert für eine hohe Bewertung liegt bei mehr als 10 Anfragen innerhalb von 30 Minuten.</p> <div data-bbox="829 527 1507 936" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Die Schwellenwerte, für die diese Regel gilt, können aufgrund der Latenz leicht variieren. Bei einigen Anfragen wird möglicherweise das Limit überschritten, bevor die Regelaktion angewendet wird.</p></div> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:acfp:aggregate:volumetric:phone_number:high</code></p> <p>Die Regelgruppe wendet die folgenden Bezeichnungen auf Anfragen mit mittlerem Volumen (6-10 Anfragen pro 30-Minuten-Fenster) und geringem Volumen (2-5 Anfragen pro 30-Minuten-Fenster) an, ergreift jedoch keine Maßnahmen dafür: <code>aws:waf:managed:aws:acfp:aggregate:volumetric:phone_number:medium</code> und <code>aws:waf:managed:aws:acfp:aggregate:volumetric:phone_number:low</code></p>

Regelname	Beschreibung und Kennzeichnung
VolumetricAddressHigh	<p>Prüft auf große Mengen von Anfragen zur Kontoerstellung, die dieselbe physische Adresse verwenden. Der Schwellenwert für eine hohe Bewertung liegt bei mehr als 100 Anfragen pro 30-Minuten-Fenster.</p> <div data-bbox="829 527 1507 936"><p> Note</p><p>Die Schwellenwerte, für die diese Regel gilt, können aufgrund der Latenz leicht variieren. Bei einigen Anfragen wird möglicherweise das Limit überschritten, bevor die Regelaktion angewendet wird.</p></div> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:acfp:aggregate:volumetric:address:high</p>



Regelname	Beschreibung und Kennzeichnung
VolumetricAddressLow	<p>Prüft auf geringe und mittlere Mengen von Anfragen zur Kontoerstellung, die dieselbe physische Adresse verwenden. Der Schwellenwert für eine mittlere Bewertung liegt bei mehr als 51-100 Anfragen pro 30-Minuten-Fenster und bei einer niedrigen Bewertung bei 11-50 Anfragen pro 30-Minuten-Fenster.</p> <p>Die Regel wendet die Aktion entweder für mittlere oder niedrige Volumen an.</p> <div data-bbox="829 747 1508 1157" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Die Schwellenwerte, für die diese Regel gilt, können aufgrund der Latenz leicht variieren. Bei einigen Anfragen wird möglicherweise das Limit überschritten, bevor die Regelaktion angewendet wird.</p></div> <p>Regelaktion: CAPTCHA</p> <p>Bezeichnung: <code>awswaf:managed:aws:acfp:aggregate:volumetric:address:low</code> oder <code>awswaf:managed:aws:acfp:aggregate:volumetric:address:medium</code></p>


Regelname	Beschreibung und Kennzeichnung
VolumetricIPSuccessfulResponse	<p>Prüft, ob eine große Anzahl erfolgreicher Anfragen zur Kontoerstellung für eine einzelne IP-Adresse vorliegt. Diese Regel fasst erfolgreiche Antworten von der geschützten Ressource auf Anfragen zur Kontoerstellung zusammen. Der Schwellenwert für eine hohe Bewertung liegt bei mehr als 10 Anfragen pro 10-Minuten-Fenster.</p> <p>Diese Regel schützt vor Versuchen, Konten massenweise zu erstellen. Sie hat einen niedrigeren Schwellenwert als die Regel <code>VolumetricIpHigh</code>, bei der nur die Anfragen gezählt werden.</p> <p>Wenn Sie die Regelgruppe so konfiguriert haben, dass sie den Antworttext oder die JSON-Komponenten überprüft, AWS WAF können Sie die ersten 65.536 Byte (64 KB) dieser Komponententypen auf Erfolgs- oder Fehlerindikatoren überprüfen.</p> <p>Diese Regel wendet die Regelaktion und -kennzeichnung auf neue Webanfragen von einer IP-Adresse an und basiert auf den Erfolgs- und Fehlschlagantworten der geschützten Ressource auf die letzten Anmeldeversuche von derselben IP-Adresse aus. Bei der Konfiguration der Regelgruppe legen Sie fest, wie Erfolge und Misserfolge gezählt werden.</p>

Regelname	Beschreibung und Kennzeichnung
	<p data-bbox="857 247 1507 478"> Note AWS WAF wertet diese Regel nur in Web-ACLs aus, die CloudFront Amazon-Distributionen schützen.</p> <p data-bbox="857 573 1507 1077"> Note Die Schwellenwerte, für die diese Regel gilt, können aufgrund der Latenz leicht variieren. Es ist möglich, dass der Client mehr erfolgreiche Versuche zur Kontoerstellung sendet, als zulässig sind, bevor die Regel bei nachfolgenden Versuchen mit dem Abgleich beginnt.</p> <p data-bbox="829 1182 1097 1213">Regelaktion: Block</p> <p data-bbox="829 1262 1443 1392">Label: <code>awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:high</code></p> <p data-bbox="829 1440 1458 1856">Die Regelgruppe wendet außerdem die folgenden verwandten Bezeichnungen auf Anfragen an, ohne dass eine entsprechende Aktion ausgeführt wird. Alle Zählungen beziehen sich auf ein Zeitfenster von 10 Minuten. <code>awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:medium</code> für mehr als 5 erfolgrei</p>

Regelname	Beschreibung und Kennzeichnung
	<p>che Anfragen, <code>aws:waf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:low</code> für mehr als eine erfolgreiche Anfrage, <code>aws:waf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:high</code> für mehr als 10 fehlgeschlagene Anfragen, <code>aws:waf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:medium</code> für mehr als 5 fehlgeschlagene Anfragen und <code>aws:waf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:low</code> für mehr als eine fehlgeschlagene Anfrage.</p>

Regelname	Beschreibung und Kennzeichnung
VolumetricSessionSuccessful Response	<p>Überprüft, ob die geschützte Ressource nur wenige erfolgreiche Antworten auf Anfragen zur Kontoerstellung gesendet hat, die von einer einzelnen Clientsitzung aus gesendet wurden. Dies trägt zum Schutz vor Versuchen zur Erstellung mehrerer Konten bei. Der Schwellenwert für eine niedrige Bewertung liegt bei mehr als 1 Anfrage pro 30-Minuten-Fenster.</p> <p>Dies schützt vor Versuchen, Konten in großen Mengen zu erstellen. Diese Regel verwendet einen niedrigeren Schwellenwert als die Regel <code>VolumetricSessionHigh</code>, die nur die Anfragen verfolgt.</p> <p>Wenn Sie die Regelgruppe so konfiguriert haben, dass sie den Antworttext oder die JSON-Komponenten überprüft, AWS WAF können Sie die ersten 65.536 Byte (64 KB) dieser Komponententypen auf Erfolgs- oder Fehlerindikatoren überprüfen.</p> <p>Diese Regel wendet die Regelaktion und -kennzeichnung auf neue Webanfragen aus einer Clientsitzung an und basiert auf den Erfolgs- und Fehlschlagantworten der geschützten Ressource auf die letzten Anmeldeversuche aus derselben Clientsitzung. Bei der Konfiguration der Regelgruppe legen Sie fest, wie Erfolge und Fehlschläge gezählt werden.</p>

Regelname	Beschreibung und Kennzeichnung
	<p data-bbox="857 247 982 283"> Note</p> <p data-bbox="906 304 1393 430">AWS WAF wertet diese Regel nur in Web-ACLs aus, die CloudFront Amazon-Distributionen schützen.</p> <p data-bbox="857 613 982 648"> Note</p> <p data-bbox="906 669 1477 1039">Die Schwellenwerte, für die diese Regel gilt, können aufgrund der Latenz leicht variieren. Es ist möglich, dass der Client mehr fehlgeschlagene Versuche zur Kontoerstellung sendet, als zulässig sind, bevor die Regel bei nachfolgenden Versuchen mit dem Abgleich beginnt.</p> <p data-bbox="824 1180 1096 1215">Regelaktion: Block</p> <p data-bbox="824 1260 1445 1396">Label: <code>aws:waf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:low</code></p> <p data-bbox="824 1438 1494 1856">Die Regelgruppe wendet außerdem die folgenden verwandten Bezeichnungen auf Anfragen an. Alle Zählungen beziehen sich auf ein Zeitfenster von 30 Minuten. <code>aws:waf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:high</code> für mehr als 10 erfolgreiche Anfragen, <code>aws:waf:managed:aws:acfp:aggregate:vo</code></p>

Regelname	Beschreibung und Kennzeichnung
	<p>lumetric:session:successful_creation_response:medium für mehr als 5 erfolgreiche Anfragen, awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:high für mehr als 10 fehlgeschlagene Anfragen, awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:medium für mehr als 5 fehlgeschlagene Anfragen und awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:low für mehr als eine fehlgeschlagene Anfrage.</p>
VolumetricSessionTokenReuseIp	<p>Prüft Anfragen zur Kontoerstellung auf die Verwendung eines einzelnen Tokens unter mehr als 5 verschiedenen IP-Adressen.</p> <div data-bbox="829 1136 1507 1545" style="border: 1px solid #add8e6; border-radius: 15px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>Die Schwellenwerte, für die diese Regel gilt, können aufgrund der Latenz leicht variieren. Bei einigen Anfragen wird möglicherweise das Limit überschritten, bevor die Regelaktion angewendet wird.</p> </div> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:token_reuse:ip</p>

AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen (ATP) zur Betrugsbekämpfung

VendorName:AWS, Name:AWSManagedRulesATPRuleSet, WCU: 50

Die verwaltete Regelgruppe zur Verhinderung von Kontoübernahmen (AWS WAF Fraud Control Account Takeover Prevention, ATP) kennzeichnet und verwaltet Anfragen, die Teil böswilliger Kontoübernahmeversuche sein könnten. Zu diesem Zweck untersucht die Regelgruppe Anmeldeversuche, die Clients an den Anmeldeendpunkt Ihrer Anwendung senden.

- **Überprüfung von Anfragen** — ATP bietet Ihnen Transparenz und Kontrolle über ungewöhnliche Anmeldeversuche und Anmeldeversuche, bei denen gestohlene Anmeldeinformationen verwendet werden, um Kontoübernahmen zu verhindern, die zu betrügerischen Aktivitäten führen könnten. ATP überprüft E-Mail- und Passwortkombinationen anhand seiner Datenbank mit gestohlenen Anmeldeinformationen, die regelmäßig aktualisiert wird, sobald neue durchgesickerte Anmeldeinformationen im Dark Web gefunden werden. ATP aggregiert Daten nach IP-Adresse und Clientsitzung, um Clients zu erkennen und zu blockieren, die zu viele Anfragen verdächtiger Art senden.
- **Überprüfung der Antworten** — Bei CloudFront Verteilungen untersucht die ATP-Regelgruppe nicht nur eingehende Anmeldeanfragen, sondern auch die Antworten Ihrer Anwendung auf Anmeldeversuche, um Erfolgs- und Fehlschlagquoten nachzuverfolgen. Mithilfe dieser Informationen kann ATP vorübergehend Clientsitzungen oder IP-Adressen blockieren, bei denen zu viele Anmeldefehler aufgetreten sind. AWS WAF führt die Antwortprüfung asynchron durch, sodass die Latenz Ihres Webverkehrs dadurch nicht erhöht wird.

Verwenden Sie diese Regelgruppe

Diese Regelgruppe erfordert eine spezielle Konfiguration. Anleitungen zur Konfiguration und Implementierung dieser Regelgruppe finden Sie unter [AWS WAF Verhinderung von Kontoübernahmen bei der Betrugsbekämpfung \(ATP\)](#).

Diese Regelgruppe ist Teil der intelligenten Schutzmaßnahmen zur Abwehr von Bedrohungen in. AWS WAF Weitere Informationen finden Sie unter [AWS WAF intelligente Bedrohungsabwehr](#).

Note

Wenn Sie diese verwaltete Regelgruppe verwenden, werden Ihnen zusätzliche Gebühren berechnet. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).

Um Ihre Kosten niedrig zu halten und sicherzustellen, dass Sie Ihren Web-Traffic nach Ihren Wünschen verwalten, verwenden Sie diese Regelgruppe gemäß den Anweisungen unter [Bewährte Methoden für intelligente Bedrohungsabwehr](#).

Diese Regelgruppe ist nicht für die Verwendung mit Amazon Cognito Cognito-Benutzerpools verfügbar. Sie können eine Web-ACL, die diese Regelgruppe verwendet, keinem Benutzerpool zuordnen, und Sie können diese Regelgruppe nicht zu einer Web-ACL hinzufügen, die bereits einem Benutzerpool zugeordnet ist.

Diese Regelgruppe bietet keine Versionsverwaltungs- oder SNS-Aktualisierungsbenachrichtigungen.

Von dieser Regelgruppe hinzugefügte Labels

Diese verwaltete Regelgruppe fügt den Webanforderungen, die sie auswertet, Labels hinzu, die für Regeln verfügbar sind, die nach dieser Regelgruppe in Ihrer Web-ACL ausgeführt werden. AWS WAF zeichnet die Labels auch anhand von CloudWatch Amazon-Metriken auf. Allgemeine Informationen zu Labels und Label-Metriken finden Sie unter [Bezeichnungen bei Webanforderungen](#) und [Kennzeichnen Sie Metriken und Dimensionen](#).

Token-Labels


Diese Regelgruppe verwendet AWS WAF Tokenverwaltung, um Webanfragen anhand des Status ihrer AWS WAF Token zu überprüfen und zu kennzeichnen. AWS WAF verwendet Token für die Nachverfolgung und Überprüfung von Clientsitzungen.

Hinweise zu Token und Tokenverwaltung finden Sie unter [AWS WAF Webanforderungstoken](#).

Informationen zu den hier beschriebenen Label-Komponenten finden Sie unter [Bezeichnungssyntax- und Benennungsanforderungen](#).

Bezeichnung der Clientsitzung

Das Label `aws:waf:managed:token:id:identifizier` enthält eine eindeutige Kennung, anhand derer die AWS WAF Tokenverwaltung die Clientsitzung identifiziert. Die Kennung kann sich ändern, wenn der Client ein neues Token erwirbt, beispielsweise nachdem er das Token, das er verwendet hat, verworfen hat.

 Note

AWS WAF meldet keine CloudWatch Amazon-Metriken für dieses Label.

Token-Statusbezeichnungen: Namespace-Präfixe für Labels

Token-Statusbezeichnungen berichten über den Status des Tokens und der darin enthaltenen Challenge- und CAPTCHA-Informationen.

Jedes Token-Statuslabel beginnt mit einem der folgenden Namespace-Präfixe:

- `awsaf:managed:token:`— Wird verwendet, um den allgemeinen Status des Tokens und den Status der Challenge-Informationen des Tokens zu melden.
- `awsaf:managed:captcha:`— Wird verwendet, um über den Status der CAPTCHA-Informationen des Tokens zu berichten.

Token-Statusbezeichnungen: Labelnamen

Nach dem Präfix enthält der Rest des Labels detaillierte Informationen zum Token-Status:

- `accepted`— Das Anforderungstoken ist vorhanden und enthält Folgendes:
 - Eine gültige Challenge oder CAPTCHA-Lösung.
 - Eine noch nicht abgelaufene Herausforderung oder ein CAPTCHA-Zeitstempel.
 - Eine Domainspezifikation, die für die Web-ACL gültig ist.

Beispiel: Das Label `awsaf:managed:token:accepted` gibt an, dass das Token der Webanfragen eine gültige Challenge-Lösung, einen noch nicht abgelaufenen Challenge-Zeitstempel und eine gültige Domain enthält.

- `rejected`— Das Anforderungstoken ist vorhanden, erfüllt aber nicht die Akzeptanzkriterien.

Zusammen mit dem abgelehnten Label fügt die Tokenverwaltung einen benutzerdefinierten Label-Namespace und einen Namen hinzu, um den Grund anzugeben.

- `rejected:not_solved`— Dem Token fehlt die Challenge- oder CAPTCHA-Lösung.
- `rejected:expired`— Der Challenge- oder CAPTCHA-Zeitstempel des Tokens ist gemäß den von Ihrer Web-ACL konfigurierten Token-Immunitätszeiten abgelaufen.
- `rejected:domain_mismatch`— Die Domain des Tokens entspricht nicht der Token-Domain-Konfiguration Ihrer Web-ACL.
- `rejected:invalid`— Das angegebene Token AWS WAF konnte nicht gelesen werden.

Beispiel: Die Labels `awsaf:managed:captcha:rejected` und `awsaf:managed:captcha:rejected:expired` geben an, dass die Anfrage abgelehnt wurde,

weil der CAPTCHA-Zeitstempel im Token die in der Web-ACL konfigurierte CAPTCHA-Token-Immunitätszeit überschritten hat.

- `absent`— Die Anfrage hat das Token nicht oder der Token-Manager konnte es nicht lesen.

Beispiel: Das Label `aws:waf:managed:captcha:absent` gibt an, dass die Anfrage das Token nicht enthält.

ATP-Etiketten

Die von ATP verwaltete Regelgruppe generiert Labels mit dem Namespace-Präfix, `aws:waf:managed:aws:atp:` gefolgt vom benutzerdefinierten Namespace und dem Labelnamen.

Die Regelgruppe kann zusätzlich zu den Bezeichnungen, die in der Regelliste aufgeführt sind, eines der folgenden Labels hinzufügen:

- `aws:waf:managed:aws:atp:signal:credential_compromised`— Zeigt an, dass sich die Anmeldeinformationen, die in der Anfrage übermittelt wurden, in der Datenbank mit gestohlenen Anmeldeinformationen befinden.
- `aws:waf:managed:aws:atp:aggregate:attribute:suspicious_tls_fingerprint`— Nur für geschützte CloudFront Amazon-Distributionen verfügbar. Zeigt an, dass eine Clientsitzung mehrere Anfragen gesendet hat, bei denen ein verdächtiger TLS-Fingerabdruck verwendet wurde.
- `aws:waf:managed:aws:atp:aggregate:volumetric:session:token_reuse:ip`— Weist auf die Verwendung eines einzelnen Tokens unter mehr als 5 verschiedenen IP-Adressen hin. Die Schwellenwerte, für die diese Regel gilt, können aufgrund der Latenz leicht variieren. Bei einigen Anfragen wird möglicherweise das Limit überschritten, bevor das Etikett angewendet wird.

Sie können alle Labels für eine Regelgruppe über die API abrufen, indem Sie `DescribeManagedRuleGroup` aufrufen. Die Kennzeichnungen werden in der Eigenschaft `AvailableLabels` in der Antwort aufgeführt.

Liste der Regeln zur Verhinderung von Kontoübernahmen


In diesem Abschnitt sind die ATP-Regeln `AWSManagedRulesATPRuleSet` und die Bezeichnungen aufgeführt, die die Regeln der Regelgruppe Webanfragen hinzufügen.

Note

Die Informationen, die wir für die Regeln in den Regelgruppen „AWS Verwaltete Regeln“ veröffentlichen, sollen Ihnen genügend Informationen zur Verfügung stellen, um die Regeln zu verwenden, ohne dass böswillige Akteure die Regeln umgehen könnten. Wenn Sie mehr Informationen benötigen, als Sie in dieser Dokumentation finden, wenden Sie sich an das [AWS Support Center](#).

Regelname	Beschreibung und Kennzeichnung
UnsupportedCognitoIDP	<p>Prüft, ob Web-Traffic an einen Amazon Cognito Cognito-Benutzerpool gesendet wird. ATP ist nicht für die Verwendung mit Amazon Cognito Cognito-Benutzerpools verfügbar, und diese Regel trägt dazu bei, dass die anderen ATP-Regelgruppenregeln nicht zur Auswertung des Benutzerpool-Traffics verwendet werden.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:atp:unsupported:cognito_idp</code></p>
VolumetricIpHigh	<p>Prüft auf eine hohe Anzahl von Anforderungen, die von einzelnen IP-Adressen gesendet werden. Ein hohes Volumen umfasst mehr als 20 Anfragen in einem 10-Minuten-Fenster.</p> <div data-bbox="829 1476 1507 1885" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p>Note</p> <p>Die Schwellenwerte, für die diese Regel gilt, können aufgrund der Latenz leicht variieren. Bei einem hohen Volumen können einige Anfragen das Limit überschreiten, bevor die Regelaktion angewendet wird.</p> </div>



Regelname	Beschreibung und Kennzeichnung
	<p data-bbox="829 243 1094 279">Regelaktion: Block</p> <p data-bbox="829 323 1443 407">Label: <code>aws:waf:managed:aws:atp:aggregate:volumetric:ip:high</code></p> <p data-bbox="829 451 1479 915">Die Regelgruppe wendet die folgenden Bezeichnungen auf Anfragen mit mittlerem Volumen (16-20 Anfragen pro 10-Minuten-Fenster) und geringem Volumen (11-15 Anfragen pro 10-Minuten-Fenster) an, ergreift jedoch keine Maßnahmen dafür: <code>aws:waf:managed:aws:atp:aggregate:volumetric:ip:medium</code> und <code>aws:waf:managed:aws:atp:aggregate:volumetric:ip:low</code></p>

Regelname	Beschreibung und Kennzeichnung
VolumetricSession	<p>Prüft auf große Mengen von Anfragen, die aus einzelnen Clientsitzungen gesendet wurden. Der Schwellenwert liegt bei mehr als 20 Anfragen pro 30-Minuten-Fenster.</p> <p>Diese Inspektion gilt nur, wenn die Webanforderung über ein Token verfügt. Token werden Anfragen durch die Anwendungsintegrations-SDKs und durch die Regelaktionen CAPTCHA und Challenge hinzugefügt. Weitere Informationen finden Sie unter AWS WAF Webanforderungstoken.</p> <div data-bbox="829 842 1508 1255" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Die Schwellenwerte, für die diese Regel gilt, können aufgrund der Latenz leicht variieren. Bei einigen Anfragen wird möglicherweise das Limit überschritten, bevor die Regelaktion angewendet wird.</p></div> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:atp:aggregate:volumetric:session</code></p>

Regelname	Beschreibung und Kennzeichnung
AttributeCompromisedCredentials	<p>Sucht nach mehreren Anfragen aus derselben Clientsitzung, die gestohlene Anmeldeinformationen verwenden.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:atp:aggregate:attribute:compromised_credentials</code></p>
AttributeUsernameTraversal	<p>Prüft, ob mehrere Anfragen aus derselben Clientsitzung stammen und die Benutzernamendurchquerung verwenden.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:atp:aggregate:attribute:username_traversal</code></p>
AttributePasswordTraversal	<p>Prüft, ob mehrere Anfragen aus derselben Clientsitzung stammen und die Kennwortüberschreitung verwenden.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:atp:aggregate:attribute:password_traversal</code></p>



Regelname	Beschreibung und Kennzeichnung
AttributeLongSession	<p>Prüft, ob mehrere Anfragen aus derselben Clientsitzung stammen, für die lang andauernde Sitzungen verwendet werden.</p> <p>Diese Prüfung gilt nur, wenn die Webanforderung über ein Token verfügt. Token werden Anfragen durch die Anwendungsintegrations-SDKs und durch die Regelaktionen CAPTCHA und Challenge hinzugefügt. Weitere Informationen finden Sie unter AWS WAF Webanforderungstoken.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:atp:aggregate:attribute:long_session</code></p>
TokenRejected	<p>Prüft auf Anfragen mit Tokens, die von der AWS WAF Tokenverwaltung abgelehnt wurden.</p> <p>Diese Inspektion gilt nur, wenn die Webanforderung ein Token enthält. Token werden Anfragen durch die Anwendungsintegrations-SDKs und durch die Regelaktionen CAPTCHA und Challenge hinzugefügt. Weitere Informationen finden Sie unter AWS WAF Webanforderungstoken.</p> <p>Regelaktion: Block</p> <p>Bezeichnung: Keine. Um zu überprüfen, ob das Token zurückgewiesen wurde, verwenden Sie eine Label-Abgleichsregel, um den Abgleich auf dem Etikett vorzunehmen: <code>aws:waf:managed:token:rejected</code></p>

Regelname	Beschreibung und Kennzeichnung
SignalMissingCredential	<p>Prüft auf Anfragen mit Anmeldeinformationen, bei denen der Benutzername oder das Passwort fehlt.</p> <p>Regelaktion: Block</p> <p>Label: <code>awswaf:managed:aws:atp:signal:missing_credential</code></p>

Regelname	Beschreibung und Kennzeichnung
VolumetricIpFailedLoginResponseHigh	<p data-bbox="829 260 1495 531">Sucht nach IP-Adressen, die in letzter Zeit die Ursache für eine zu hohe Anzahl fehlgeschlagener Anmeldeversuche waren. Ein hohes Volumen besteht aus mehr als 10 fehlgeschlagenen Anmeldeanfragen von einer IP-Adresse innerhalb eines Zeitfensters von 10 Minuten.</p> <p data-bbox="829 579 1446 850">Wenn Sie die Regelgruppe so konfiguriert haben, dass sie den Antworttext oder die JSON-Komponenten überprüft, AWS WAF können Sie die ersten 65.536 Byte (64 KB) dieser Komponententypen auf Erfolgs- oder Fehlerindikatoren überprüfen.</p> <p data-bbox="829 898 1511 1262">Diese Regel wendet die Regelaktion und -kennzeichnung auf neue Webanfragen von einer IP-Adresse an und basiert auf den Erfolgs- und Fehlschlagantworten der geschützten Ressource auf die letzten Anmeldeversuche von derselben IP-Adresse aus. Bei der Konfiguration der Regelgruppe legen Sie fest, wie Erfolge und Misserfolge gezählt werden.</p> <div data-bbox="829 1304 1507 1570"><p data-bbox="862 1346 976 1377"> Note</p><p data-bbox="906 1402 1393 1528">AWS WAF wertet diese Regel nur in Web-ACLs aus, die CloudFront Amazon-Distributionen schützen.</p></div> <div data-bbox="829 1671 1507 1850"><p data-bbox="862 1713 976 1745"> Note</p><p data-bbox="906 1770 1463 1850">Die Schwellenwerte, für die diese Regel gilt, können aufgrund der Latenz</p></div>

Regelname	Beschreibung und Kennzeichnung
	<p>leicht variieren. Es ist möglich, dass der Client mehr fehlgeschlagene Anmeldeversuche sendet, als zulässig sind, bevor die Regel bei nachfolgenden Versuchen mit dem Abgleich beginnt.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high</code></p> <p>Die Regelgruppe wendet außerdem die folgenden verwandten Bezeichnungen auf Anfragen an, ohne dass eine Aktion damit verknüpft ist. Alle Zählungen beziehen sich auf ein Zeitfenster von 10 Minuten. <code>aws:waf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:medium</code> für mehr als 5 fehlgeschlagene Anfragen, <code>aws:waf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:low</code> für mehr als 1 fehlgeschlagene Anfrage, <code>aws:waf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:high</code> für mehr als 10 erfolgreiche Anfragen, <code>aws:waf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:medium</code> für mehr als 5 erfolgreiche Anfragen und <code>aws:waf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:low</code> für mehr als 1 erfolgreiche Anfrage.</p>

Regelname	Beschreibung und Kennzeichnung
	<code>p:successful_login_response:low</code> für mehr als 1 erfolgreiche Anfrage.

Regelname	Beschreibung und Kennzeichnung
VolumetricSessionFailedLoginsResponseHigh	<p>Sucht nach Clientsitzungen, die in letzter Zeit zu viele fehlgeschlagene Anmeldeversuche verursacht haben. Ein hohes Volumen besteht aus mehr als 10 fehlgeschlagenen Anmeldeanfragen aus einer Clientsitzung innerhalb eines Zeitfensters von 30 Minuten.</p> <p>Wenn Sie die Regelgruppe so konfiguriert haben, dass sie den Antworttext oder die JSON-Komponenten überprüft, AWS WAF können Sie die ersten 65.536 Byte (64 KB) dieser Komponententypen auf Erfolgs- oder Fehlerindikatoren überprüfen.</p> <p>Diese Regel wendet die Regelaktion und -kennzeichnung auf neue Webanfragen aus einer Clientsitzung an und basiert auf den Erfolgs- und Fehlschlagantworten der geschützten Ressource auf die letzten Anmeldeversuche aus derselben Clientsitzung. Bei der Konfiguration der Regelgruppe legen Sie fest, wie Erfolge und Misserfolge gezählt werden.</p> <div data-bbox="829 1304 1507 1570"><p> Note</p><p>AWS WAF wertet diese Regel nur in Web-ACLs aus, die CloudFront Amazon-Distributionen schützen.</p></div> <div data-bbox="829 1671 1507 1850"><p> Note</p><p>Die Schwellenwerte, für die diese Regel gilt, können aufgrund der Latenz</p></div>

Regelname	Beschreibung und Kennzeichnung
	<p>leicht variieren. Es ist möglich, dass der Client mehr fehlgeschlagene Anmeldeversuche sendet, als zulässig sind, bevor die Regel bei nachfolgenden Versuchen mit dem Abgleich beginnt.</p> <p>Diese Prüfung gilt nur, wenn die Webanforderung ein Token enthält. Token werden Anfragen durch die Anwendungsintegrations-SDKs und durch die Regelaktionen CAPTCHA und Challenge hinzugefügt. Weitere Informationen finden Sie unter AWS WAF Webanforderungstoken.</p> <p>Regelaktion: Block</p> <p>Label: <code>awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:high</code></p> <p>Die Regelgruppe wendet außerdem die folgenden verwandten Bezeichnungen auf Anfragen an, ohne dass eine Aktion damit verknüpft ist. Alle Zählungen beziehen sich auf ein 30-Minuten-Fenster. <code>awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:medium</code> für mehr als 5 fehlgeschlagene Anfragen, <code>awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:low</code> für mehr als 1 fehlgeschlagene Anfrage, <code>awswaf:managed:aws</code></p>

Regelname	Beschreibung und Kennzeichnung
	<p>:atp:aggregate:volumetric:session:successful_login_response:high für mehr als 10 erfolgreiche Anfragen, awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:medium für mehr als 5 erfolgreiche Anfragen und awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:low für mehr als 1 erfolgreiche Anfrage.</p>

AWS WAF Regelgruppe „Bot-Kontrolle“

VendorName:AWS, Name:AWSManagedRulesBotControlRuleSet, WCU: 50

Die von Bot Control verwaltete Regelgruppe stellt Regeln zur Verwaltung von Anfragen von Bots bereit. Bots können überschüssige Ressourcen verbrauchen, Geschäftskennzahlen verfälschen, Ausfallzeiten verursachen und böswillige Aktivitäten ausführen.

Schutzstufen

Die von Bot Control verwaltete Regelgruppe bietet zwei Schutzstufen, aus denen Sie wählen können:

- **Allgemein** — Erkennt eine Vielzahl von sich selbst identifizierenden Bots, z. B. Web-Scraping-Frameworks, Suchmaschinen und automatisierte Browser. Bot-Control-Schutzmaßnahmen auf dieser Ebene identifizieren häufig auftretende Bots mithilfe herkömmlicher Bot-Erkennungstechniken, wie z. B. der Analyse statischer Anforderungsdaten. Die Regeln kennzeichnen den Traffic dieser Bots und blockieren diejenigen, die sie nicht verifizieren können.
- **Gezielt** — Beinhaltet Schutzmaßnahmen auf allgemeiner Ebene und bietet eine gezielte Erkennung für ausgeklügelte Bots, die sich nicht selbst identifizieren. Gezielte Schutzmaßnahmen reduzieren Bot-Aktivitäten mithilfe einer Kombination aus Ratenbegrenzung und CAPTCHA sowie Browser-Herausforderungen im Hintergrund.

- **TGT_**— Regeln, die gezielten Schutz bieten, haben Namen, die mit **TGT_** beginnen. Alle gezielten Schutzmaßnahmen verwenden Erkennungstechniken wie Browserabfragen, Fingerabdrücke und Verhaltensheuristiken, um bösartigen Bot-Traffic zu identifizieren.
- **TGT_ML_**— Gezielte Schutzregeln, die maschinelles Lernen verwenden, haben Namen, die mit **TGT_ML_** beginnen. Diese Regeln verwenden automatisierte, maschinelle Lernanalysen der Besucherstatistiken von Websites, um ungewöhnliches Verhalten zu erkennen, das auf verteilte, koordinierte Bot-Aktivitäten hindeutet. AWS WAF analysiert Statistiken über Ihren Website-Verkehr wie Zeitstempel, Browsereigenschaften und die zuvor besuchte URL, um das maschinelle Lernmodell von Bot Control zu verbessern. Funktionen für maschinelles Lernen sind standardmäßig aktiviert, Sie können sie jedoch in Ihrer Regelgruppenkonfiguration deaktivieren. Wenn maschinelles Lernen deaktiviert ist, werden diese Regeln von AWS WAF nicht ausgewertet.

Sowohl die angestrebte Schutzstufe als auch die AWS WAF ratenbasierte Regelaussage bieten eine Ratenbegrenzung. Einen Vergleich der beiden Optionen finden Sie unter [Optionen zur Ratenbegrenzung in ratenbasierten Regeln und gezielten Bot-Kontrollregeln](#)

Diese Regelgruppe verwenden

Diese Regelgruppe ist Teil der intelligenten Schutzmaßnahmen zur Abwehr von Bedrohungen in AWS WAF. Weitere Informationen finden Sie unter [AWS WAF intelligente Bedrohungsabwehr](#).

Note

Wenn Sie diese verwaltete Regelgruppe verwenden, werden Ihnen zusätzliche Gebühren berechnet. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).

Um Ihre Kosten niedrig zu halten und sicherzustellen, dass Sie Ihren Web-Traffic nach Ihren Wünschen verwalten, verwenden Sie diese Regelgruppe gemäß den Anweisungen unter [Bewährte Methoden für intelligente Bedrohungsabwehr](#).

Wir aktualisieren regelmäßig unsere Modelle für maschinelles Lernen (ML) für die angestrebte Schutzstufe, um die ML-basierten Regeln zu verbessern, um die Bot-Vorhersagen zu verbessern. Die Namen der ML-basierten Regeln beginnen mit **TGT_ML_**. Wenn Sie eine plötzliche und wesentliche Änderung der Bot-Vorhersagen aufgrund dieser Regeln feststellen, kontaktieren Sie uns über Ihren Kundenbetreuer oder eröffnen Sie einen Fall im [AWS Support Center](#).

Die Regelgruppe Bot Control bietet keine Benachrichtigungen über SNS-Updates.

Von dieser Regelgruppe hinzugefügte Labels

Diese verwaltete Regelgruppe fügt den Webanforderungen, die sie auswertet, Labels hinzu, die für Regeln verfügbar sind, die nach dieser Regelgruppe in Ihrer Web-ACL ausgeführt werden. AWS WAF zeichnet die Labels auch anhand von CloudWatch Amazon-Metriken auf. Allgemeine Informationen zu Labels und Label-Metriken finden Sie unter [Bezeichnungen bei Webanforderungen](#) und [Kennzeichnen Sie Metriken und Dimensionen](#).

Token-Labels

Diese Regelgruppe verwendet AWS WAF Tokenverwaltung, um Webanfragen anhand des Status ihrer AWS WAF Token zu überprüfen und zu kennzeichnen. AWS WAF verwendet Token für die Nachverfolgung und Überprüfung von Clientsitzungen.

Hinweise zu Token und Tokenverwaltung finden Sie unter [AWS WAF Webanforderungstoken](#).

Informationen zu den hier beschriebenen Label-Komponenten finden Sie unter [Bezeichnungssyntax- und Benennungsanforderungen](#).

Bezeichnung der Clientsitzung

Das Label `awsfaf:managed:token:id:identifizier` enthält eine eindeutige Kennung, anhand derer die AWS WAF Tokenverwaltung die Clientsitzung identifiziert. Die Kennung kann sich ändern, wenn der Client ein neues Token erwirbt, beispielsweise nachdem er das Token, das er verwendet hat, verworfen hat.

Note

AWS WAF meldet keine CloudWatch Amazon-Metriken für dieses Label.

Token-Statusbezeichnungen: Namespace-Präfixe für Labels

Token-Statusbezeichnungen berichten über den Status des Tokens und der darin enthaltenen Challenge- und CAPTCHA-Informationen.

Jedes Token-Statuslabel beginnt mit einem der folgenden Namespace-Präfixe:

- `awsfaf:managed:token:`— Wird verwendet, um den allgemeinen Status des Tokens und den Status der Challenge-Informationen des Tokens zu melden.

- `aws:waf:managed:captcha:`— Wird verwendet, um über den Status der CAPTCHA-Informationen des Tokens zu berichten.

Token-Statusbezeichnungen: Labelnamen

Nach dem Präfix enthält der Rest des Labels detaillierte Informationen zum Token-Status:

- `accepted`— Das Anforderungstoken ist vorhanden und enthält Folgendes:
 - Eine gültige Challenge oder CAPTCHA-Lösung.
 - Eine noch nicht abgelaufene Herausforderung oder ein CAPTCHA-Zeitstempel.
 - Eine Domainspezifikation, die für die Web-ACL gültig ist.

Beispiel: Das Label `aws:waf:managed:token:accepted` gibt an, dass das Token der Webanfragen eine gültige Challenge-Lösung, einen noch nicht abgelaufenen Challenge-Zeitstempel und eine gültige Domain enthält.

- `rejected`— Das Anforderungstoken ist vorhanden, erfüllt aber nicht die Akzeptanzkriterien.

Zusammen mit dem abgelehnten Label fügt die Tokenverwaltung einen benutzerdefinierten Label-Namespace und einen Namen hinzu, um den Grund anzugeben.

- `rejected:not_solved`— Dem Token fehlt die Challenge- oder CAPTCHA-Lösung.
- `rejected:expired`— Der Challenge- oder CAPTCHA-Zeitstempel des Tokens ist gemäß den von Ihrer Web-ACL konfigurierten Token-Immunitätszeiten abgelaufen.
- `rejected:domain_mismatch`— Die Domain des Tokens entspricht nicht der Token-Domain-Konfiguration Ihrer Web-ACL.
- `rejected:invalid`— Das angegebene Token AWS WAF konnte nicht gelesen werden.

Beispiel: Die Labels `aws:waf:managed:captcha:rejected` und `aws:waf:managed:captcha:rejected:expired` geben an, dass die Anfrage abgelehnt wurde, weil der CAPTCHA-Zeitstempel im Token die in der Web-ACL konfigurierte CAPTCHA-Token-Immunitätszeit überschritten hat.

- `absent`— Die Anfrage hat das Token nicht oder der Token-Manager konnte es nicht lesen.

Beispiel: Das Label `aws:waf:managed:captcha:absent` gibt an, dass die Anfrage das Token nicht enthält.

Beschriftungen von Bot Control

Die von Bot Control verwaltete Regelgruppe generiert Labels mit dem Namespace-Präfix, `aws:waf:managed:aws:bot-control:` gefolgt vom benutzerdefinierten Namespace und dem Labelnamen. Die Regelgruppe kann einer Anfrage mehr als ein Label hinzufügen.

Jedes Label spiegelt die Ergebnisse der Bot-Control-Regel wider:

- `aws:waf:managed:aws:bot-control:bot:`— Informationen über den Bot, der mit der Anfrage verknüpft ist.
 - `aws:waf:managed:aws:bot-control:bot:name:<name>`— Der Bot-Name, falls einer verfügbar ist, z. B. die benutzerdefinierten Namespaces `bot:name:slurp`, `bot:name:googlebot` und `bot:name:pocket_parser`
 - `aws:waf:managed:aws:bot-control:bot:category:<category>`— Die Kategorie des Bots, wie sie AWS WAF beispielsweise durch und definiert wird. `bot:category:search_engine` `bot:category:content_fetcher`
 - `aws:waf:managed:aws:bot-control:bot:organization:<organization>`— Der Herausgeber des Bots, zum Beispiel `bot:organization:google`.
 - `aws:waf:managed:aws:bot-control:bot:verified`— Wird verwendet, um auf einen Bot hinzuweisen, der sich selbst identifiziert und den Bot Control verifizieren konnte. Dies wird für gängige wünschenswerte Bots verwendet und kann in Kombination mit Kategoriekennzeichnungen wie `bot:category:search_engine` oder Namenskennzeichnungen wie `bot:name:googlebot` nützlich sein.

Note

Bot Control verwendet die IP-Adresse aus der Herkunft der Webanfrage, um festzustellen, ob ein Bot verifiziert ist. Sie können es nicht so konfigurieren, dass es die AWS WAF weitergeleitete IP-Konfiguration verwendet, um eine andere IP-Adressquelle zu überprüfen. Wenn Sie Bots verifiziert haben, die über einen Proxy oder Load Balancer weiterleiten, können Sie zu diesem Zweck eine Regel hinzufügen, die vor der Regelgruppe Bot Control ausgeführt wird. Konfigurieren Sie Ihre neue Regel so, dass sie die weitergeleitete IP-Adresse verwendet und Anfragen von verifizierten Bots explizit zulässt. Informationen zur Verwendung weitergeleiteter IP-Adressen finden Sie unter [Weitergeleitete IP-Adresse](#).

- `aws:waf:managed:aws:bot-control:bot:user_triggered:verified`— Wird verwendet, um auf einen Bot hinzuweisen, der einem verifizierten Bot ähnelt, der aber möglicherweise direkt von Endbenutzern aufgerufen wird. Diese Bot-Kategorie wird nach den Bot-Kontrollregeln wie ein nicht verifizierter Bot behandelt.
- `aws:waf:managed:aws:bot-control:bot:developer_platform:verified`— Wird verwendet, um auf einen Bot hinzuweisen, der einem verifizierten Bot ähnelt, der aber von Entwicklerplattformen für die Skripterstellung verwendet wird, beispielsweise Google Apps Script. Diese Kategorie von Bots wird nach den Bot-Kontrollregeln wie ein nicht verifizierter Bot behandelt.
- `aws:waf:managed:aws:bot-control:bot:unverified`— Wird verwendet, um auf einen Bot hinzuweisen, der sich selbst identifiziert, sodass er benannt und kategorisiert werden kann, der aber keine Informationen veröffentlicht, anhand derer seine Identität unabhängig überprüft werden kann. Diese Arten von Bot-Signaturen können gefälscht werden und werden daher als nicht verifiziert behandelt.
- `aws:waf:managed:aws:bot-control:targeted:<additional-details>` — Wird für Labels verwendet, die spezifisch für die gezielten Schutzmaßnahmen von Bot Control sind.
- `aws:waf:managed:aws:bot-control:signal:<signal-details>` und `aws:waf:managed:aws:bot-control:targeted:signal:<signal-details>` — Wird in einigen Situationen verwendet, um zusätzliche Informationen zur Anfrage bereitzustellen.

Im Folgenden finden Sie Beispiele für Signalbezeichnungen. Diese Liste ist nicht erschöpfend:

- `aws:waf:managed:aws:bot-control:targeted:signal:browser_automation_extension`— Weist auf die Erkennung einer Browsererweiterung hin, die die Automatisierung unterstützt, z. B. Selenium IDE.

Dieses Label wird immer dann hinzugefügt, wenn ein Benutzer diese Art von Erweiterung installiert hat, auch wenn er sie nicht aktiv verwendet. Wenn Sie hierfür eine Regel zum Abgleich von Bezeichnungen implementieren, sollten Sie sich dieser Möglichkeit von Fehlalarmen in Ihrer Regellogik und Ihren Aktionseinstellungen bewusst sein. Sie könnten beispielsweise eine CAPTCHA Aktion anstelle von Label-Matches verwenden Block oder diesen Label-Abgleich mit anderen Label-Übereinstimmungen kombinieren, um Ihr Vertrauen zu erhöhen, dass Automatisierung verwendet wird.

- `aws:waf:managed:aws:bot-control:signal:automated_browser`— Weist darauf hin, dass die Anfrage Hinweise darauf enthält, dass der Client-Browser möglicherweise automatisiert ist.

- `aws:waf:managed:aws:bot-control:targeted:signal:automated_browser`— Weist darauf hin, dass das AWS WAF Token der Anfrage Hinweise darauf enthält, dass der Client-Browser automatisiert sein könnte.

Sie können alle Labels für eine Regelgruppe über die API abrufen, indem Sie `DescribeManagedRuleGroup` aufrufen. Die Kennzeichnungen werden in der Eigenschaft `AvailableLabels` in der Antwort aufgeführt.

Die von Bot Control verwaltete Regelgruppe wendet Kennzeichnungen auf eine Reihe verifizierbarer Bots an, die üblicherweise zulässig sind. Die Regelgruppe blockiert diese verifizierten Bots nicht. Wenn Sie möchten, können Sie sie oder einen Teil davon blockieren, indem Sie eine benutzerdefinierte Regel schreiben, die die Labels verwendet, die von der verwalteten Regelgruppe Bot Control zugewiesen wurden. Weitere Informationen und Beispiele finden Sie unter [AWS WAF Bot-Steuerung](#).

Liste der Bot-Control-Regeln

In diesem Abschnitt sind die Bot-Control-Regeln aufgeführt.

Note

Die Informationen, die wir für die Regeln in den Regelgruppen „AWS Verwaltete Regeln“ veröffentlichen, sollen Ihnen genügend Informationen zur Verfügung stellen, damit Sie die Regeln verwenden können, ohne dass böswillige Akteure die Regeln umgehen könnten. Wenn Sie mehr Informationen benötigen, als Sie in dieser Dokumentation finden, wenden Sie sich an das [AWS Support Center](#).

Regelname	Beschreibung
CategoryAdvertising	Prüft auf Bots, die zu Werbezwecken verwendet werden. Sie können beispielsweise Werbedienste von Drittanbietern verwenden, die programmgesteuert auf Ihre Website zugreifen müssen.

Regelname	Beschreibung
	<p>Regelaktion, die nur auf nicht verifizierte Bots angewendet wird: Block</p> <p>Label: <code>awswaf:managed:aws:bot-control:bot:category:advertising</code></p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelbezeichnung und die Bezeichnung <code>awswaf:managed:aws:bot-control:bot:verified</code> hinzu.</p>
CategoryArchiver	<p>Prüft auf Bots, die zu Archivierungszwecken verwendet werden. Diese Bots crawlen das Internet und erfassen Inhalte, um Archive zu erstellen.</p> <p>Regelaktion, die nur auf nicht verifizierte Bots angewendet wird: Block</p> <p>Label: <code>awswaf:managed:aws:bot-control:bot:category:archiver</code></p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelbezeichnung und die Bezeichnung <code>awswaf:managed:aws:bot-control:bot:verified</code> hinzu.</p>

Regelname	Beschreibung
CategoryContentFetcher	<p>Prüft nach Bots, die die Website der Anwendung im Namen eines Benutzers besuchen, um Inhalte wie RSS-Feeds abzurufen oder Ihre Inhalte zu verifizieren oder zu validieren.</p> <p>Regelaktion, die nur auf nicht verifizierte Bots angewendet wird: Block</p> <p>Label: <code>aws:waf:managed:aws:bot-control:bot:category:content_fetcher</code></p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelbezeichnung und die Bezeichnung <code>aws:waf:managed:aws:bot-control:bot:verified</code> hinzu.</p>

Regelname	Beschreibung
CategoryEmailClient	<p>Sucht nach Bots, die Links in E-Mails überprüfen, die auf die Website der Anwendung verweisen. Dazu können Bots gehören, die von Unternehmen und E-Mail-Anbietern betrieben werden, um Links in E-Mails zu verifizieren und verdächtige E-Mails zu kennzeichnen.</p> <p>Regelaktion, die nur auf nicht verifizierte Bots angewendet wird: Block</p> <p>Label: <code>aws:waf:managed:aws:bot-control:bot:category:email_client</code></p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelbezeichnung und die Bezeichnung <code>aws:waf:managed:aws:bot-control:bot:verified</code> hinzu.</p>
CategoryHttpLibrary	<p>Prüft auf Anfragen, die von Bots aus den HTTP-Bibliotheken verschiedener Programmiersprachen generiert wurden. Dazu können API-Anfragen gehören, die Sie zulassen oder überwachen möchten.</p> <p>Regelaktion, die nur auf nicht verifizierte Bots angewendet wird: Block</p> <p>Label: <code>aws:waf:managed:aws:bot-control:bot:category:http_library</code></p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelbezeichnung und die Bezeichnung <code>aws:waf:managed:aws:bot-control:bot:verified</code> hinzu.</p>

Regelname	Beschreibung
CategoryLinkChecker	<p>Prüft auf Bots, die nach defekten Links suchen.</p> <p>Regelaktion, die nur auf nicht verifizierte Bots angewendet wird: Block</p> <p>Label: <code>aws:waf:managed:aws:bot-control:bot:category:link_checker</code></p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelbezeichnung und die Bezeichnung <code>aws:waf:managed:aws:bot-control:bot:verified</code> hinzu.</p>
CategoryMiscellaneous	<p>Sucht nach verschiedenen Bots, die nicht zu anderen Kategorien passen.</p> <p>Regelaktion, gilt nur für nicht verifizierte Bots: Block</p> <p>Label: <code>aws:waf:managed:aws:bot-control:bot:category:miscellaneous</code></p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelbezeichnung und die Bezeichnung <code>aws:waf:managed:aws:bot-control:bot:verified</code> hinzu.</p>


Regelname	Beschreibung
CategoryMonitoring	<p>Prüft auf Bots, die zu Überwachungszwecken verwendet werden. Sie können beispielsweise Bot-Überwachungsdienste verwenden, die regelmäßig einen Ping-Befehl an die Website Ihrer Anwendung senden, um Dinge wie Leistung und Verfügbarkeit zu überwachen.</p> <p>Regelaktion, die nur auf nicht verifizierte Bots angewendet wird: Block</p> <p>Label: <code>aws:waf:managed:aws:bot-control:bot:category:monitoring</code></p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelbezeichnung und die Bezeichnung <code>aws:waf:managed:aws:bot-control:bot:verified</code> hinzu.</p>
CategoryScrapingFramework	<p>Sucht nach Bots aus Web-Scraping-Frameworks, die zum Automatisieren des Crawlens und Extrahieren von Inhalten von Websites verwendet werden.</p> <p>Regelaktion, die nur auf nicht verifizierte Bots angewendet wird: Block</p> <p>Label: <code>aws:waf:managed:aws:bot-control:bot:category:scraping_framework</code></p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelbezeichnung und die Bezeichnung <code>aws:waf:managed:aws:bot-control:bot:verified</code> hinzu.</p>

Regelname	Beschreibung
CategorySearchEngine	<p>Sucht nach Suchmaschinen-Bots, die Websites crawlen, um Inhalte zu indexieren und die Informationen für Suchmaschinenergebnisse verfügbar zu machen.</p> <p>Regelaktion, gilt nur für nicht verifizierte Bots: Block</p> <p>Label: <code>aws:waf:managed:aws:bot-control:bot:category:search_engine</code></p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelbezeichnung und die Bezeichnung <code>aws:waf:managed:aws:bot-control:bot:verified</code> hinzu.</p>
CategorySecurity	<p>Sucht nach Bots, die Webanwendungen auf Sicherheitslücken scannen oder Sicherheitsüberprüfungen durchführen. Sie könnten beispielsweise einen Drittanbieter für Sicherheitslösungen beauftragen, der die Sicherheit Ihrer Webanwendung scannt, überwacht oder überprüft.</p> <p>Regelaktion, die nur auf nicht verifizierte Bots angewendet wird: Block</p> <p>Label: <code>aws:waf:managed:aws:bot-control:bot:category:security</code></p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelbezeichnung und die Bezeichnung <code>aws:waf:managed:aws:bot-control:bot:verified</code> hinzu.</p>


Regelname	Beschreibung
CategorySeo	<p>Prüft auf Bots, die für die Suchmaschinenoptimierung verwendet werden. Sie könnten beispielsweise Suchmaschinentools verwenden, die Ihre Website crawlen, um Ihre Platzierungen in Suchmaschinen zu verbessern.</p> <p>Regelaktion, die nur auf nicht verifizierte Bots angewendet wird: Block</p> <p>Label: <code>aws:waf:managed:aws:bot-control:bot:category:seo</code></p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelbezeichnung und die Bezeichnung <code>aws:waf:managed:aws:bot-control:bot:verified</code> hinzu.</p>
CategorySocialMedia	<p>Sucht nach Bots, die von Social-Media-Plattformen verwendet werden, um Inhaltszusammenfassungen bereitzustellen, wenn Nutzer Ihre Inhalte teilen.</p> <p>Regelaktion, gilt nur für nicht verifizierte Bots: Block</p> <p>Label: <code>aws:waf:managed:aws:bot-control:bot:category:social_media</code></p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelbezeichnung und die Bezeichnung <code>aws:waf:managed:aws:bot-control:bot:verified</code> hinzu.</p>

Regelname	Beschreibung
CategoryAI	<p>Prüft nach Bots mit künstlicher Intelligenz (KI).</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:bot-control:bot:category:ai</code></p>
SignalAutomatedBrowser	<p>Prüft die Anfrage auf Hinweise darauf, dass der Client-Browser möglicherweise automatisiert ist. Automatisierte Browser können zum Testen oder Scraping verwendet werden. Sie können diese Browsertypen beispielsweise verwenden , um Ihre Anwendungswebsite zu überwachen oder zu verifizieren.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:bot-control:signal:automated_browser</code></p>
SignalKnownBotDataCenter	<p>Sucht nach Indikatoren für Rechenzentren, die normalerweise von Bots genutzt werden.</p> <p>Regelaktion: Block</p> <p>Label: <code>aws:waf:managed:aws:bot-control:signal:known_bot_data_center</code></p>

Regelname	Beschreibung
SignalNonBrowserUserAgent	<p>Prüft auf Benutzeragent-Zeichenfolgen, die offenbar nicht von einem Webbrowser stammen. Diese Kategorie kann API-Anfragen beinhalten.</p> <p>Regelaktion: Block</p> <p>Label: awswaf:managed:aws:bot-control:signal:non_browser_user_agent</p>

Regelname	Beschreibung
TGT_VolumetricIpTokenAbsent	<p>Prüft, ob in den letzten 5 Minuten 5 oder mehr Anfragen von einem Kunden eingegangen sind, die kein gültiges Challenge-Token enthalten. Informationen zu Tokens finden Sie unter AWS WAF Webanforderungstoken.</p> <div data-bbox="829 493 1507 997"><p> Note</p><p>Es ist möglich, dass diese Regel bei einer Anfrage mit einem Token übereinstimmt, wenn bei Anfragen desselben Clients kürzlich Token fehlten.</p><p>Der Schwellenwert, für den diese Regel gilt, kann aufgrund der Latenz leicht variieren.</p></div> <p>Diese Regel behandelt fehlende Token anders als die Token-Kennzeichnung: <code>aws:waf:managed:token:absent</code>. Das Token-Label kennzeichnet einzelne Anfragen, die kein Token haben. Diese Regel erfasst für jede Client-IP die Anzahl der Anfragen, denen ihr Token fehlt, und vergleicht sie mit Clients, die das Limit überschreiten.</p> <p>Regelaktion, die nur auf Clients angewendet wird, bei denen es sich nicht um verifizierte Bots handelt: Challenge</p> <p>Label: <code>aws:waf:managed:aws:bot-control:targeted:aggregate:volumetric:ip:token_absent</code></p>


Regelname	Beschreibung
	Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelbezeichnung und die Bezeichnung hinzu <code>aws:waf:managed:aws:bot-control:bot:verified</code> .


Regelname	Beschreibung
TGT_VolumetricSession	<p>Prüft in einem beliebigen 5-Minuten-Fenster auf eine ungewöhnlich hohe Anzahl von Anfragen aus einer Clientsitzung. Die Bewertung basiert auf einem Vergleich mit volumetrischen Standardbasislinien, bei dem historische Verkehrsmuster verwendet werden. AWS WAF</p> <p>Diese Prüfung gilt nur, wenn die Webanforderung über ein Token verfügt. Token werden Anfragen durch die Anwendungsintegrations-SDKs und durch die Regelaktionen CAPTCHA und Challenge hinzugefügt. Weitere Informationen finden Sie unter AWS WAF Webanforderungstoken.</p> <div data-bbox="829 940 1507 1396" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Es kann 5 Minuten dauern, bis diese Regel wirksam wird, nachdem Sie sie aktiviert haben. Bot Control identifiziert anomales Verhalten in Ihrem Web-Traffic, indem es den aktuellen Traffic mit den von Ihnen berechneten Traffic-Baselines vergleicht. AWS WAF</p></div> <p>Regelaktion, die nur auf Clients angewendet wird, bei denen es sich nicht um verifizierte Bots handelt: CAPTCHA</p> <p>Label: awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:high</p>


Regelname	Beschreibung
	<p>Die Regelgruppe wendet die folgenden Bezeichnungen auf Anfragen mit mittlerem und niedrigerem Volumen an, die über einem Mindestschwellenwert liegen. Für diese Stufen ergreift die Regel keine Aktion, unabhängig davon, ob der Client verifiziert ist: <code>aws:waf:managed:aws:bot-control:targeted:aggregate:volumetric:session:medium</code> und <code>aws:waf:managed:aws:bot-control:targeted:aggregate:volumetric:session:low</code> .</p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelkennzeichnung und die Bezeichnung hinzu <code>aws:waf:managed:aws:bot-control:bot:verified</code> .</p>

Regelname	Beschreibung
TGT_SignalAutomatedBrowser	<p>Überprüft das Token der Anfrage auf Anzeichen dafür, dass der Client-Browser möglicherweise automatisiert ist. Weitere Informationen finden Sie unter Token-Eigenschaften.</p> <p>Diese Überprüfung gilt nur, wenn die Webanforderung ein Token enthält. Token werden Anfragen durch die Anwendung integrations-SDKs und durch die Regelaktionen CAPTCHA und Challenge hinzugefügt. Weitere Informationen finden Sie unter AWS WAF Webanforderungstoken.</p> <p>Regelaktion, die nur auf Clients angewendet wird, bei denen es sich nicht um verifizierte Bots handelt: CAPTCHA</p> <p>Label: <code>awswaf:managed:aws:bot-control:targeted:signal:automated_browser</code></p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelbezeichnung und die Bezeichnung hinzu <code>awswaf:managed:aws:bot-control:bot:verified</code>.</p>

Regelname	Beschreibung
TGT_SignalBrowserInconsistency	<p>Prüft auf inkonsistente Browser-Abfragedaten. Weitere Informationen finden Sie unter Token-Eigenschaften.</p> <p>Diese Prüfung gilt nur, wenn die Webanforderung über ein Token verfügt. Token werden Anfragen durch die Anwendungsintegrations-SDKs und durch die Regelaktionen CAPTCHA und Challenge hinzugefügt. Weitere Informationen finden Sie unter AWS WAF Webanforderungstoken.</p> <p>Regelaktion, die nur auf Clients angewendet wird, bei denen es sich nicht um verifizierte Bots handelt: CAPTCHA</p> <p>Label: <code>awswaf:managed:aws:bot-control:targeted:signal:browser_inconsistency</code></p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelbezeichnung und die Bezeichnung <code>awswaf:managed:aws:bot-control:bot:verified</code> hinzu.</p>

Regelname	Beschreibung
TGT-TokenReuseIp	<p data-bbox="829 258 1484 338">Prüft, ob ein einzelnes Token unter mehr als 5 verschiedenen IP-Adressen verwendet wird.</p> <div data-bbox="829 384 1507 793"><p data-bbox="862 422 980 457"> Note</p><p data-bbox="907 478 1474 747">Die Schwellenwerte, für die diese Regel gilt, können aufgrund der Latenz leicht variieren. Bei einigen Anfragen wird möglicherweise das Limit überschritten, bevor die Regelaktion angewendet wird.</p></div> <p data-bbox="829 894 1105 930">Regelaktion: Count</p> <p data-bbox="829 974 1442 1104">Label: awswaf:managed:aws:bot-control:targeted:aggregate:volume:session:token_reuse:ip</p>

Regelname	Beschreibung
TGT_ML_CoordinatedActivityMedium und TGT_ML_CoordinatedActivityHigh	<p>Suchen Sie nach anomalen Verhaltensweisen, die auf verteilte, koordinierte Bot-Aktivitäten zurückzuführen sind. Die Regelstufen geben an, mit welcher Sicherheit eine Gruppe von Anfragen an einem koordinierten Angriff beteiligt ist.</p> <div data-bbox="829 573 1508 1031" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Diese Regeln werden nur ausgeführt, wenn die Regelgruppe für maschinelles Lernen (ML) konfiguriert ist. Informationen zur Konfiguration dieser Auswahl finden Sie unter Hinzufügen der von AWS WAF Bot Control verwalteten Regelgruppe zu Ihrer Web-ACL.</p></div> <p>AWS WAF führt diese Inspektion durch maschinelles Lernen durch, indem Statistiken zum Website-Traffic analysiert werden. AWS WAF analysiert den Webverkehr alle paar Minuten und optimiert die Analyse für die Erkennung von Bots mit geringer Intensität und langer Dauer, die über viele IP-Adressen verteilt sind.</p> <p>Diese Regeln stimmen möglicherweise bei einer sehr kleinen Anzahl von Anfragen überein, bevor festgestellt wird, dass kein koordinierter Angriff im Gange ist. Wenn Sie also nur eine oder zwei Übereinstimmungen sehen, sind die Ergebnisse möglicherweise falsch positiv. Wenn Sie jedoch feststellen,</p>

Regelname	Beschreibung
	<p>dass viele Spiele aufgrund dieser Regeln auftreten, handelt es sich wahrscheinlich um einen koordinierten Angriff.</p> <div data-bbox="829 384 1507 1171" style="border: 1px solid #add8e6; border-radius: 15px; padding: 15px;"><p> Note</p><p>Es kann bis zu 24 Stunden dauern, bis diese Regeln in Kraft treten, nachdem Sie die gezielten Bot-Control-Regeln mit der ML-Option aktiviert haben. Bot Control identifiziert ungewöhnliches Verhalten in Ihrem Web-Traffic, indem es den aktuellen Traffic mit den berechneten Traffic-Baselines vergleicht. AWS WAF AWS WAF berechnet nur die Baselines, wenn Sie die gezielten Regeln von Bot Control mit der ML-Option verwenden. Die Erstellung aussagekräftiger Baselines kann bis zu 24 Stunden dauern.</p></div> <p>Wir aktualisieren unsere Modelle für maschinelles Lernen regelmäßig für diese Regeln, um die Bot-Vorhersagen zu verbessern. Wenn Sie eine plötzliche und wesentliche Änderung der Bot-Vorhersagen, die diese Regeln enthalten, feststellen, wenden Sie sich an Ihren Kundenbetreuer oder eröffnen Sie einen Fall im AWS Support Center.</p> <p>Regelaktionen, die nur auf Kunden angewendet werden, bei denen es sich nicht um verifizierte Bots handelt:</p> <ul style="list-style-type: none">•

Regelname	Beschreibung
	<p>Medium: Count</p> <ul style="list-style-type: none"> Hoch: Count <p>Labels: <code>awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:medium</code> und <code>awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:high</code></p> <p>Bei verifizierten Bots ergreift die Regelgruppe keine Maßnahmen, fügt jedoch die Regelkennzeichnung und die Bezeichnung hinzu <code>awswaf:managed:aws:bot-control:bot:verified</code> .</p> <p>Die Regelgruppe fügt das Label auch hinzu, <code>awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low</code> um auf ein niedriges Konfidenzniveau hinzuweisen, wendet jedoch keine Regel an und ergreift keine Maßnahmen für diese Anfragen.</p>

Bereitstellungen für versionierte Regelgruppen mit AWS verwalteten Regeln

AWS implementiert Änderungen an seinen versionierten Regelgruppen für AWS verwaltete Regeln in drei Standardbereitstellungen: Release Candidate, statische Version und Standardversion. Darüber hinaus muss AWS manchmal eine Ausnahmereitstellung freigeben oder eine Standardversion rückgängig gemacht werden.

Note

Dieser Abschnitt gilt nur für Regelgruppen mit AWS verwalteten Regeln, die versioniert sind. Bei den Regelgruppen, die nicht versioniert sind, handelt es sich um IP-Reputation-, Bot-Control-, ATP- und ACFP-Regelgruppen.

Melden Sie sich für Bereitstellungsbenachrichtigungen an

AWS Stellt für jede Bereitstellung einer versionierten Regelgruppe mindestens eine SNS-Benachrichtigung bereit. In einigen Fällen aktualisieren wir auch die Beschreibung der verwalteten Regelgruppe in diesem Handbuch, das Änderungsprotokoll für die Regelgruppen mit AWS verwalteten Regeln und die Seite mit dem Dokumentverlauf. Informationen zur Registrierung für Benachrichtigungen finden Sie unter [Erhalten von Benachrichtigungen zu neuen Versionen und Aktualisierungen einer verwalteten Regelgruppe](#).

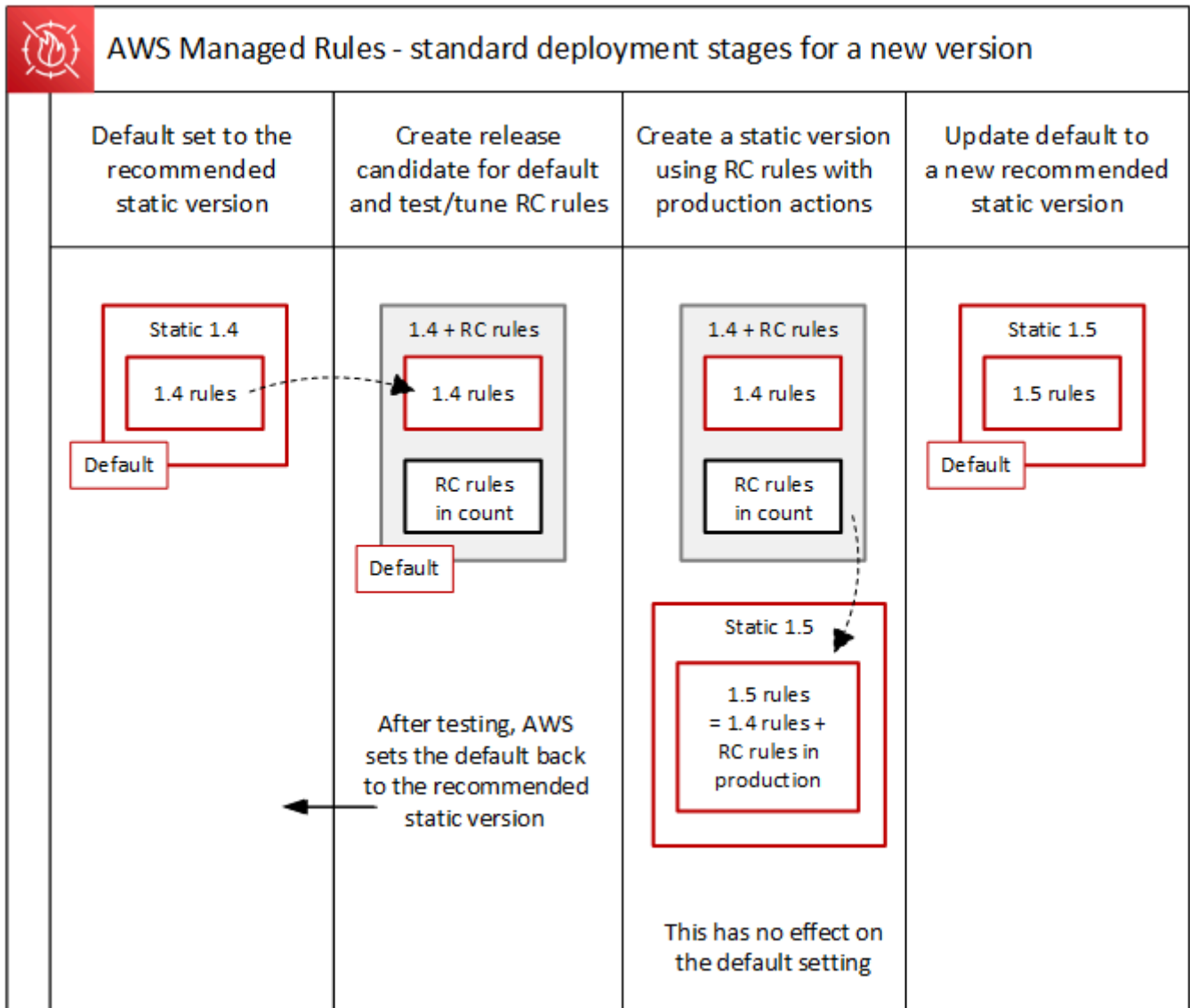
Themen

- [Überblick über die Standardbereitstellungen für AWS Managed Rules](#)
- [Typische Versionsstatus für AWS verwaltete Regeln](#)
- [Bereitstellungskandidaten für AWS Managed Rules veröffentlichen](#)
- [Statische Versionsbereitstellungen für AWS verwaltete Regeln](#)
- [Bereitstellungen von Standardversionen für AWS verwaltete Regeln](#)
- [Ausnahmebereitstellungen für AWS verwaltete Regeln](#)
- [Standard-Bereitstellungs-Rollbacks für AWS verwaltete Regeln](#)

Überblick über die Standardbereitstellungen für AWS Managed Rules

AWS führt neue Funktionen für AWS verwaltete Regeln mithilfe von drei Standardbereitstellungsphasen ein: Release Candidate, statische Version und Standardversion.

Das folgende Diagramm zeigt diese Standardbereitstellungen. Jede davon wird in den folgenden Abschnitten ausführlicher beschrieben.

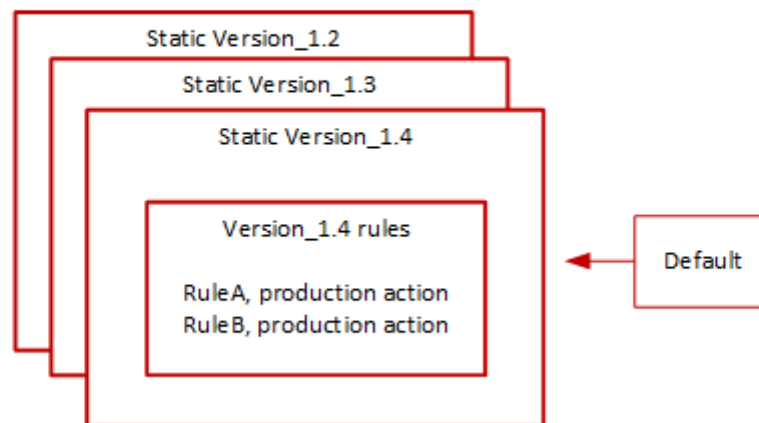


Typische Versionsstatus für AWS verwaltete Regeln

Normalerweise hat eine versionierte verwaltete Regelgruppe eine Reihe nicht abgelaufener statischer Versionen, und die Standardversion verweist auf die statische Version, AWS die empfohlen wird. Die folgende Abbildung zeigt ein Beispiel für den typischen Satz statischer Versionen und die Standardversionseinstellung.



Managed rule group: Version settings



Die Produktionsaktion für die meisten Regeln in einer statischen Version ist Block, aber sie kann auf etwas anderes gesetzt sein. Ausführliche Informationen zu den Einstellungen für Regelaktionen finden Sie in den Regellisten für jede Regelgruppe unter [AWS Liste der Regelgruppen für verwaltete Regeln](#).

Bereitstellungskandidaten für AWS Managed Rules veröffentlichen

Wenn AWS sich ein möglicher Regelsatz für eine verwaltete Regelgruppe ändert, werden diese in einer temporären Release-Candidate-Bereitstellung getestet. AWS bewertet die Kandidatenregeln im Zählmodus anhand des Produktionsdatenverkehrs und führt die letzten Optimierungsmaßnahmen durch, einschließlich der Minimierung von Fehlalarmen. AWS testet Release-Kandidatenregeln auf diese Weise für alle Kunden, die die Standardversion der Regelgruppe verwenden. Release-Candidate-Bereitstellungen gelten nicht für Kunden, die eine statische Version der Regelgruppe verwenden.

Wenn Sie die Standardversion verwenden, ändert eine Bereitstellung von Release Candidate nichts daran, wie Ihr Web-Traffic von der Regelgruppe verwaltet wird. Möglicherweise stellen Sie beim Testen der Kandidatenregeln Folgendes fest:

- Änderung des Standardversionsnamens von Default (using Version_X.Y) zu Default (using Version_X.Y_PLUS_RC_COUNT).
- Zusätzliche Zählmetriken bei Amazon CloudWatch mit RC_COUNT ihren Namen. Diese werden anhand der Release-Candidate-Regeln generiert.

AWS testet einen Release Candidate etwa eine Woche lang, entfernt ihn dann und setzt die Standardversion auf die aktuell empfohlene statische Version zurück.

AWS führt die folgenden Schritte für eine Release-Candidate-Bereitstellung durch:

1. Den Release Candidate erstellen — AWS fügt einen Release Candidate hinzu, der auf der aktuell empfohlenen statischen Version basiert, also der Version, auf die die Standardversion verweist.

Der Name des Release Candidate ist der statische Versionsname, dem Folgendes angehängt wird. `_PLUS_RC_COUNT` Wenn beispielsweise die aktuell empfohlene statische Version `Version_2.1`, würde der Release-Kandidat benannt `Version_2.1_PLUS_RC_COUNT` werden.

Der Release Candidate enthält die folgenden Regeln:

- Die Regeln wurden exakt aus der aktuell empfohlenen statischen Version kopiert, ohne dass die Regelkonfigurationen geändert wurden.
- Bieten Sie neue Regeln an, bei denen die Regelaktion auf festgelegt ist `Count` und deren Namen auf `enden_RC_COUNT`.

Die meisten Kandidatenregeln enthalten Vorschläge zur Verbesserung von Regeln, die bereits in der Regelgruppe existieren. Der Name für jede dieser Regeln ist der Name der bestehenden Regel, angehängt mit `_RC_COUNT`.

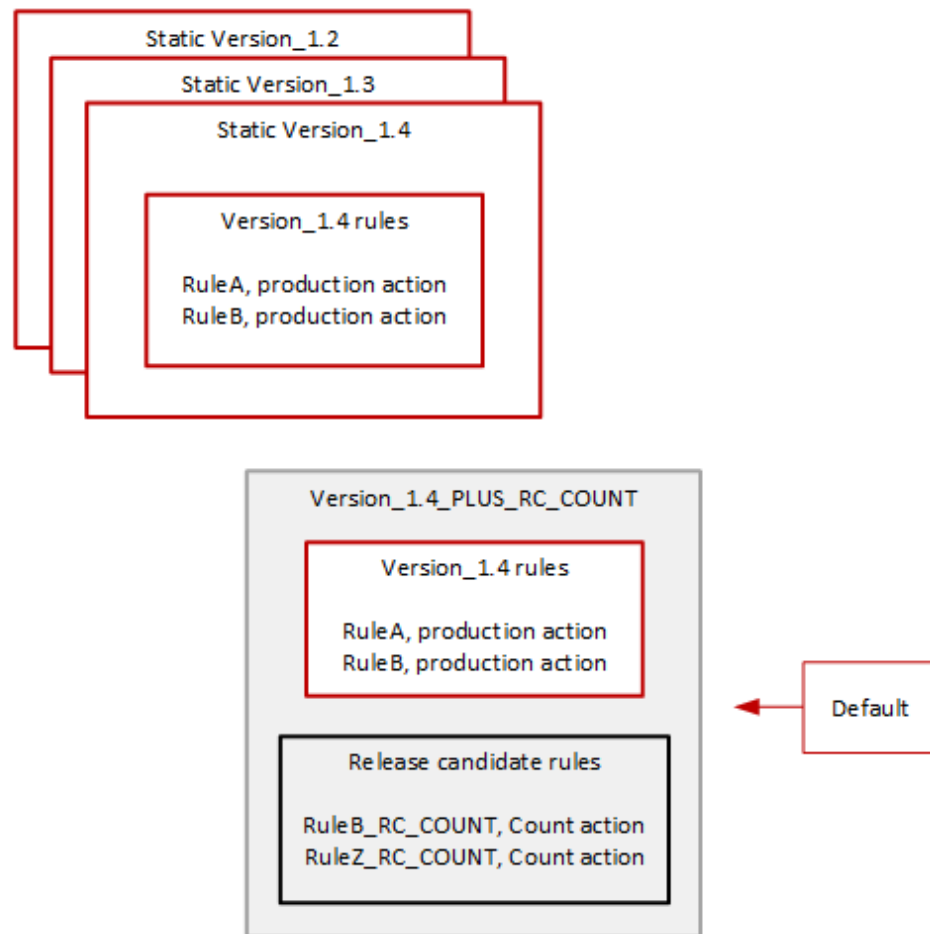
2. Legen Sie die Standardversion auf den Release Candidate fest und testen Sie — AWS legt fest, dass die Standardversion auf den neuen Release Candidate verweist, um Tests anhand Ihres Produktionsdatenverkehrs durchzuführen. Das Testen dauert in der Regel etwa eine Woche.

Sie werden feststellen, dass sich der Name der Standardversion von dem Namen, der nur die statische Version angibt, zu einem Namen `Default` (`using Version_1.4`), der die statische Version und die Release-Candidate-Regeln angibt, wie `Default` (`using Version_1.4_PLUS_RC_COUNT`) z. Anhand dieses Benennungsschemas können Sie identifizieren, welche statische Version Sie zur Verwaltung Ihres Web-Traffics verwenden.

Das folgende Diagramm zeigt den aktuellen Status der Versionen der Beispielregelgruppen.



Managed rule group: Versions with added release candidate



Die Release-Candidate-Regeln sind immer mit Count Aktionen konfiguriert, sodass sie nichts daran ändern, wie die Regelgruppe den Web-Traffic verwaltet.

Die Release-Candidate-Regeln generieren CloudWatch Amazon-Zählmetriken, AWS anhand derer das Verhalten überprüft und Fehlalarme identifiziert werden. AWS nimmt bei Bedarf Anpassungen vor, um das Verhalten der Regeln für die Anzahl der Veröffentlichungskandidaten zu optimieren.

Die Release Candidate-Version ist keine statische Version, und Sie können sie nicht aus der Liste der statischen Regelgruppenversionen auswählen. In der Standardversionsspezifikation können Sie nur den Namen der Release Candidate-Version sehen.

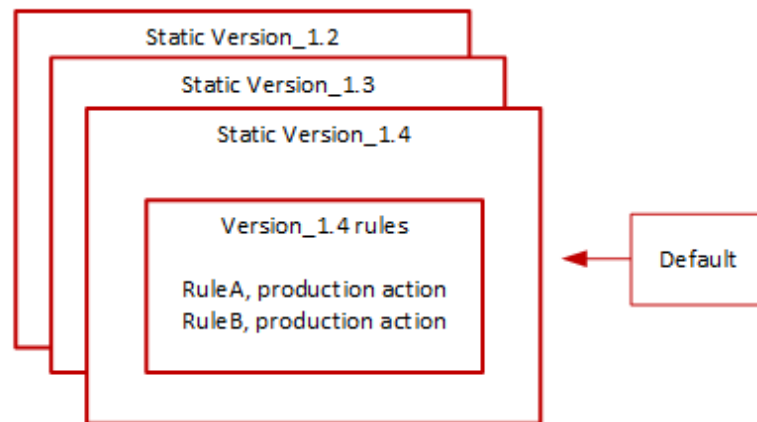
3. Setzen Sie die Standardversion auf die empfohlene statische Version zurück — Nach dem Testen der Release-Candidate-Regeln wird die Standardversion auf die aktuell empfohlene statische Version AWS zurückgesetzt. Bei der Einstellung für den Standardversionsnamen wird die `_PLUS_RC_COUNT` Endung gelöscht, und die Regelgruppe generiert keine CloudWatch

Zählmetriken mehr für die Release-Candidate-Regeln. Dies ist eine unbeaufsichtigte Änderung und nicht dasselbe wie die Bereitstellung eines Rollbacks für die Standardversion.

Das folgende Diagramm zeigt den Status der Versionen der Beispielregelgruppen nach Abschluss der Tests des Release Candidate.



Managed rule group: Release candidate testing complete



Zeitpunkt und Benachrichtigungen

AWS stellt nach Bedarf Release-Kandidatenversionen bereit, um Verbesserungen an einer Regelgruppe zu testen.

- SNS — AWS sendet zu Beginn der Bereitstellung eine SNS-Benachrichtigung. Die Benachrichtigung gibt an, wie lange der Release Candidate voraussichtlich getestet wird. Wenn der Test abgeschlossen ist AWS, wird ohne weitere Benachrichtigung automatisch die Standardeinstellung auf die statische Version zurückgesetzt.
- Änderungsprotokoll — aktualisiert das Änderungsprotokoll oder andere Teile dieses Handbuchs für diese Art der Bereitstellung AWS nicht.

Statische Versionsbereitstellungen für AWS verwaltete Regeln

Wenn AWS feststellt, dass ein Release-Kandidat wertvolle Änderungen an der Regelgruppe vornimmt, AWS wird auf der Grundlage des Release-Kandidaten eine neue statische Version für die Regelgruppe bereitgestellt. Durch diese Bereitstellung wird die Standardversion der Regelgruppe nicht geändert.

Die neue statische Version enthält die folgenden Regeln aus dem Release Candidate:

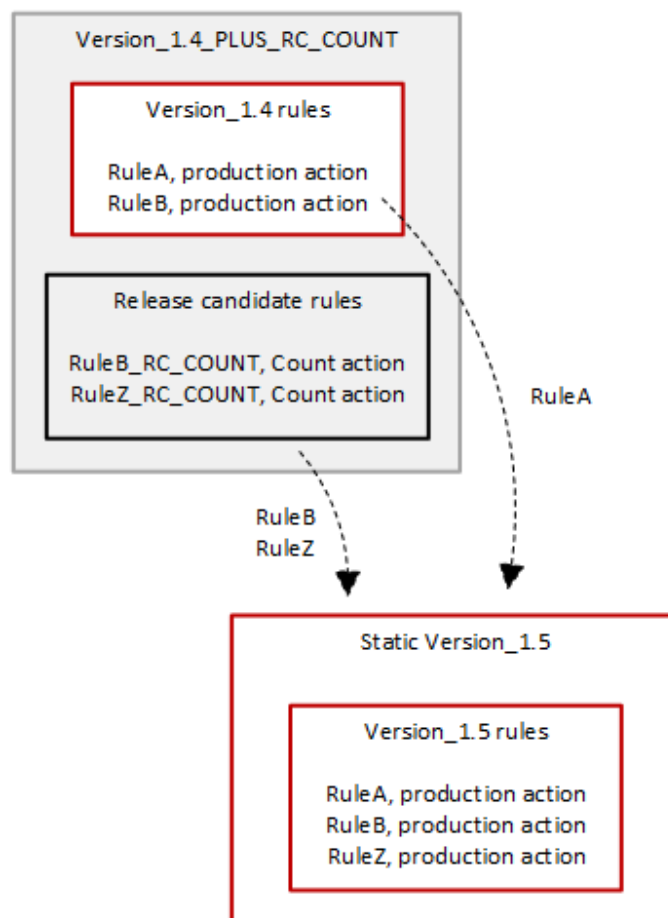
- Regeln aus der vorherigen statischen Version, für die es unter den Release-Candidate-Regeln keinen Ersatzkandidaten gibt.
- Regeln für Release-Kandidaten mit den folgenden Änderungen:
 - AWS ändert den Regelnamen, indem das Release Candidate-Suffix `_RC_COUNT` entfernt wird.
 - AWS ändert die Regelaktionen von Count zu ihren Produktionsregelaktionen.

Bei Release-Candidate-Regeln, die frühere bestehende Regeln ersetzen, ersetzt dies die Funktionalität der vorherigen Regeln in der neuen statischen Version.

Das folgende Diagramm zeigt die Erstellung der neuen statischen Version anhand des Release Candidate.



Managed rule group: Create a new static version with tested release candidate rules



Nach der Bereitstellung steht Ihnen die neue statische Version zum Testen und zur Verwendung in Ihren Schutzmaßnahmen zur Verfügung, wenn Sie möchten. Sie können neue und aktualisierte

Regelaktionen und Beschreibungen in den Regellisten der Regelgruppe unter [AWS Liste der Regelgruppen für verwaltete Regeln](#) nachlesen.

Eine statische Version ist nach der Bereitstellung unveränderlich und ändert sich nur, wenn sie AWS abläuft. Hinweise zu den Lebenszyklen von Versionen finden Sie unter [Versionsverwaltung mit verwalteten Regelgruppen](#).

Zeitablauf und Benachrichtigungen

AWS stellt bei Bedarf eine neue statische Version bereit, um die Regelgruppenfunktionalität zu verbessern. Die Bereitstellung einer statischen Version hat keinen Einfluss auf die Standardversionseinstellung.

- SNS — AWS sendet zu Beginn der Bereitstellung eine SNS-Benachrichtigung.
- Änderungsprotokoll — Sobald die Bereitstellung an allen verfügbaren Orten abgeschlossen AWS WAF ist, AWS aktualisiert die Regelgruppendefinition in diesem Handbuch nach Bedarf und kündigt die Veröffentlichung anschließend im Änderungsprotokoll der Regelgruppe für AWS verwaltete Regeln und auf der Seite mit dem Dokumentationsverlauf an.

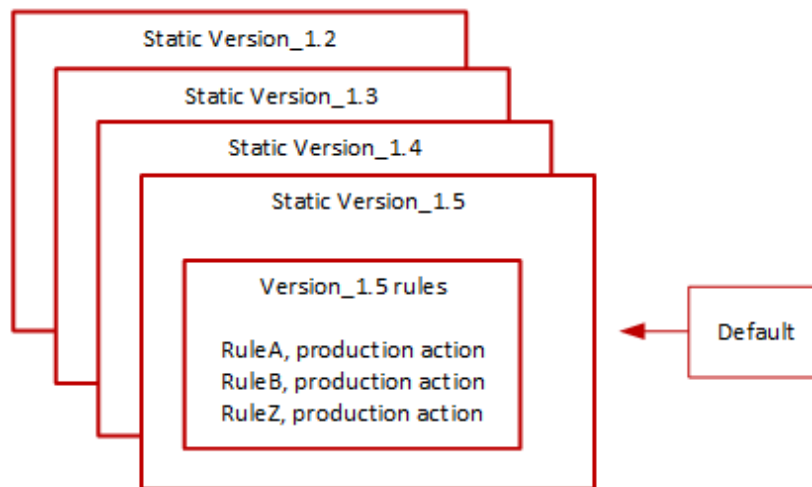
Bereitstellungen von Standardversionen für AWS verwaltete Regeln

Wenn AWS feststellt, dass eine neue statische Version im Vergleich zur aktuellen Standardversion einen verbesserten Schutz für die Regelgruppe bietet, AWS aktualisiert die Standardversion auf die neue statische Version. AWS veröffentlicht möglicherweise mehrere statische Versionen, bevor eine Version zur Standardversion der Regelgruppe heraufgestuft wird.

Das folgende Diagramm zeigt den Status der Beispielregelgruppenversionen nach dem AWS Verschieben der Standardversionseinstellung auf die neue statische Version.



Managed rule group: Update the default to a new recommended static version



AWS stellt vor der Implementierung dieser Änderung in der Standardversion Benachrichtigungen bereit, sodass Sie die bevorstehenden Änderungen testen und sich darauf vorbereiten können. Wenn Sie die Standardversion verwenden, können Sie keine Maßnahmen ergreifen und diese während des Updates beibehalten. Wenn Sie stattdessen den Wechsel zur neuen Version verzögern möchten, bevor die Bereitstellung der Standardversion geplant ist, können Sie Ihre Regelgruppe explizit so konfigurieren, dass sie die statische Version verwendet, auf die die Standardversion festgelegt ist.

Zeitpunkt und Benachrichtigungen

AWS aktualisiert die Standardversion, wenn sie eine andere statische Version für die Regelgruppe empfiehlt als die, die derzeit verwendet wird.

- **SNS** — AWS sendet mindestens eine Woche vor dem geplanten Bereitstellungstag eine SNS-Benachrichtigung und dann eine weitere am Bereitstellungstag, zu Beginn der Bereitstellung. Jede Benachrichtigung enthält den Namen der Regelgruppe, die statische Version, auf die die Standardversion aktualisiert wird, das Bereitstellungsdatum und den geplanten Zeitpunkt der Bereitstellung für jede AWS Region, in der das Update durchgeführt wird.
- **Änderungsprotokoll** — AWS Das Änderungsprotokoll oder andere Teile dieses Handbuchs für diese Art der Bereitstellung werden nicht aktualisiert.

Ausnahmebereitstellungen für AWS verwaltete Regeln

AWS könnten die Standardbereitstellungsphasen umgehen, um schnell Updates bereitzustellen, die kritische Sicherheitsrisiken beheben. Eine Ausnahmebereitstellung kann alle Standardbereitstellungstypen umfassen und sie kann schnell in allen AWS Regionen eingeführt werden.

AWS informiert so früh wie möglich über Ausnahmebereitstellungen.

Zeitplan und Benachrichtigungen

AWS führt Ausnahmebereitstellungen nur bei Bedarf durch.

- SNS — AWS sendet eine SNS-Benachrichtigung so weit wie möglich vor dem geplanten Bereitstellungstag und dann eine weitere zu Beginn der Bereitstellung. Jede Benachrichtigung enthält den Namen der Regelgruppe, die vorgenommene Änderung und das Bereitstellungsdatum.
- Änderungsprotokoll — Wenn es sich um eine statische Version handelt, AWS aktualisiert die Regelgruppendefinition in diesem Handbuch nach Abschluss der Bereitstellung an allen verfügbaren Stellen nach Bedarf und kündigt die Veröffentlichung anschließend im Änderungsprotokoll der Regelgruppe für AWS verwaltete Regeln und auf der Seite mit dem Dokumentationsverlauf an. AWS WAF

Standard-Bereitstellungs-Rollbacks für AWS verwaltete Regeln

Unter bestimmten Bedingungen AWS kann es sein, dass die Standardversion auf ihre vorherige Einstellung zurückgesetzt wird. Ein Rollback dauert in der Regel für alle AWS Regionen weniger als zehn Minuten.

AWS führt ein Rollback nur durch, um ein schwerwiegendes Problem in einer statischen Version zu beheben, z. B. ein unannehmbar hohes Maß an Fehlalarmen.

Beschleunigt nach dem Rollback der Standardversionseinstellung sowohl den Ablauf der AWS statischen Version, bei der das Problem auftritt, als auch die Veröffentlichung einer neuen statischen Version, um das Problem zu beheben.

Zeitpunkt und Benachrichtigungen

AWS führt Rollbacks der Standardversion nur bei Bedarf durch.

- SNS — AWS sendet zum Zeitpunkt des Rollbacks eine einzige SNS-Benachrichtigung. Die Benachrichtigung enthält den Namen der Regelgruppe, die Version, auf die die Standardversion

eingestellt ist, und das Bereitstellungsdatum. Dieser Bereitstellungstyp ist sehr schnell, sodass die Benachrichtigung keine Zeitinformationen für Regionen enthält.

- Änderungsprotokoll — AWS Das Änderungsprotokoll oder andere Teile dieses Handbuchs für diese Art der Bereitstellung werden nicht aktualisiert.

AWS Haftungsausschluss für verwaltete Regeln

AWS Verwaltete Regeln wurden entwickelt, um Sie vor gängigen Internet-Bedrohungen zu schützen. Wenn sie gemäß der Dokumentation verwendet werden, bieten Regelgruppen mit AWS verwalteten Regeln eine weitere Sicherheitsebene für Ihre Anwendungen. Regelgruppen mit AWS verwalteten Regeln sind jedoch nicht als Ersatz für Ihre Sicherheitsaufgaben gedacht, die durch die von Ihnen ausgewählten AWS Ressourcen bestimmt werden. Anhand des [Modells der gemeinsamen Verantwortung](#) können Sie sicherstellen, dass Ihre Ressourcen ordnungsgemäß geschützt AWS sind.

AWS Changelog für verwaltete Regeln

In diesem Abschnitt sind die Änderungen der AWS verwalteten Regeln AWS WAF seit ihrer Veröffentlichung im November 2019 aufgeführt.

Note

In diesem Changelog werden Änderungen an den Regeln und Regelgruppen in AWS Managed Rules for AWS WAF gemeldet.

In diesem Änderungsprotokoll werden Änderungen an den Regeln und der Regelgruppe sowie signifikante Änderungen an den Quellen der von den Regeln verwendeten IP-Adresslisten gemeldet. [IP-Reputationsregelgruppen](#) Änderungen an den IP-Adresslisten selbst werden nicht gemeldet, da diese Listen dynamisch sind. Wenn Sie Fragen zu den IP-Adresslisten haben, wenden Sie sich an Ihren Kundenbetreuer oder eröffnen Sie einen Fall im [AWS Support Center](#).

Regelgruppe und Regeln	Beschreibung	Datum
Amazon IP-Reputationsliste <ul style="list-style-type: none"> • AWSManagedIPReputationList 	Die Quellen der IP-Reputationsliste wurden aktualisiert, um Adressen besser identifizieren zu können, die aktiv an	2024-03-13

Regelgruppe und Regeln	Beschreibung	Datum
	<p>böswilligen Aktivitäten beteiligt sind, und um Fehlalarme zu reduzieren.</p> <p>Dieses Update beinhaltet keine neue Version, da diese Regelgruppe nicht versioniert ist.</p>	
Verwaltete Regelgruppe „Known Bad Inputs“	<p>Die statische Version 1.21 dieser Regelgruppe wurde veröffentlicht.</p> <p>Signaturen wurden hinzugefügt, um die Erkennung zu verbessern und Fehlalarme zu reduzieren.</p>	2023-12-16

Regelgruppe und Regeln	Beschreibung	Datum
<p>Verwaltete Regelgruppe „Known Bad Inputs“</p> <ul style="list-style-type: none"> ExploitablePaths_U RIPATH 	<p>Die statische Version 1.20 dieser Regelgruppe wurde veröffentlicht.</p> <p>Die ExploitablePaths_U RIPATH Regel wurde aktualisiert, sodass nun auch Anfragen erkannt werden, die der Sicherheitsanfälligkeit CVE-2023-22518 von Atlassian Confluence in Bezug auf unsachgemäße Autorisierung entsprechen. Diese Sicherheitslücke betrifft alle Versionen von Confluence Data Center und Server. Weitere Informationen finden Sie unter NIST: National Vulnerability Database: CVE-2023-22518 Detail.</p>	2023-12-14
<p>Verwaltete Regelgruppe „Core Rule Set“ (CRS)</p> <ul style="list-style-type: none"> CrossSiteScripting* 	<p>Die statische Version 1.11 dieser Regelgruppe wurde veröffentlicht.</p> <p>Allen Cross-Site-Scripting-Regeln wurden Signaturen hinzugefügt, um die Erkennung zu verbessern und Fehlalarme zu reduzieren.</p>	2023-12-06

Regelgruppe und Regeln	Beschreibung	Datum
<p>AWS WAF Regelgruppe „Bot-Kontrolle“</p> <ul style="list-style-type: none"> Neues Etikett: <code>aws:waf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low</code> 	<p>Die Bezeichnung „Koordinierte Aktivität niedrig“ wurde den Bezeichnungen für die Schutzstufe „Zielgruppe“ der Regelgruppe hinzugefügt. Dieses Label ist keiner Regel zugeordnet. Diese Kennzeichnung gilt zusätzlich zu den Regeln und Bezeichnungen auf mittlerer und hoher Ebene.</p>	2023-12-05
<p>Beschriftungen von Bot Control</p> <ul style="list-style-type: none"> Label: <code>aws:waf:managed:aws:bot-control:targeted:signal:browser_automation_extension</code> 	<p>Der Regelgruppe wurde eine Signalbezeichnung hinzugefügt, die auf die Erkennung einer Browsererweiterung hinweist, die die Automatisierung unterstützt. Diese Bezeichnung ist nicht spezifisch für eine einzelne Regel.</p>	2023-11-14
<p>Verwaltete Regelgruppe „Core Rule Set“ (CRS)</p> <ul style="list-style-type: none"> EC2MetaDataSSRF_QUERYARGUMENTS 	<p>Die statische Version 1.10 dieser Regelgruppe wurde veröffentlicht.</p> <p>Eine Regel wurde aktualisiert, um die Erkennung zu verbessern und Fehlalarme zu reduzieren.</p>	2023-11-02

Regelgruppe und Regeln	Beschreibung	Datum
<p>Verwaltete Regelgruppe „Core Rule Set“ (CRS)</p> <ul style="list-style-type: none"> • EC2MetaDataSSRF_BODY • EC2MetaDataSSRF_COOKIE • EC2MetaDataSSRF_URI_PATH • EC2MetaDataSSRF_QUERY_ARGUMENTS 	<p>Die statische Version 1.9 dieser Regelgruppe wurde veröffentlicht.</p> <p>Die Regeln wurden aktualisiert, um die Erkennung zu verbessern und Fehlalarme zu reduzieren.</p>	2023-10-30
<p>Verwaltete Regelgruppe „POSIX Operating System“</p> <ul style="list-style-type: none"> • UNIXShellCommandsVariables_QUERY_ARGUMENTS 	<p>Die statische Version 2.1 dieser Regelgruppe wurde veröffentlicht.</p> <p>Die Regel für Abfrageargumente wurde aktualisiert, um die Erkennung zu verbessern.</p>	2023-10-12

Regelgruppe und Regeln	Beschreibung	Datum
Verwaltete Regelgruppe „Core Rule Set“ (CRS) <ul style="list-style-type: none">GenericLFI_QUERYARGUMENTSGenericLFI_URI_PATHRestrictedExtensions_URI_PATHRestrictedExtensions_QUERYARGUMENTS	<p>Die statische Version 1.8 dieser Regelgruppe wurde veröffentlicht.</p> <p>Die Regeln wurden aktualisiert, um die Erkennung zu verbessern.</p>	2023-10-11

Regelgruppe und Regeln	Beschreibung	Datum
<p>Verwaltete Regelgruppe „Known Bad Inputs“</p> <ul style="list-style-type: none">ExploitablePaths_U RIPATH	<p>Bereitstellung von Ausnahmen : Die statische Version 1.19 dieser Regelgruppe wurde veröffentlicht. Die Standardversion wurde aktualisiert, sodass sie Version 1.19 verwendet.</p> <p>Die ExploitablePaths_U RIPATH Regel wurde aktualisiert, sodass nun auch Anfragen erkannt werden, die der Sicherheitslücke CVE-2023-22515 in Atlassian Confluence in Bezug auf Privilege Escalation entsprechen. Diese Sicherheitslücke betrifft einige Versionen von Atlassian Confluence. Weitere Informationen findest du unter NIST: National Vulnerability Database: CVE-2023-22515 Detail und Atlassian Support: Häufig gestellte Fragen zu CVE-2023-22515.</p> <p>Informationen zu diesem Ausnahmebereitstellungen für AWS verwaltete Regeln Bereitstellungstyp findest du unter.</p>	2023-10-04

Regelgruppe und Regeln	Beschreibung	Datum
<p>Verwaltete Regelgruppe „Known Bad Inputs“</p> <ul style="list-style-type: none"> • Host_localhost_HEADER • Log4J* • JavaDeserializatio n* 	<p>Bereitstellung von Ausnahmen : Die statische Version 1.18 dieser Regelgruppe wurde veröffentlicht. Dies ist ein schneller Rollout dieser statischen Version, um der Erstellung und Einführung von Version 1.19 Rechnung zu tragen.</p> <p>Die Host_localhost_HEADER Regel und alle Log4J- und Java-Deserialisierungsregeln wurden aktualisiert, um die Erkennung zu verbessern.</p> <p>Hinweise zu diesem Bereitstellungstyp finden Sie unter. Ausnahmebereitstellungen für AWS verwaltete Regeln</p>	2023-10-04

Regelgruppe und Regeln	Beschreibung	Datum
AWS WAF Regelgruppe „Bot-Kontrolle“ <ul style="list-style-type: none"> • TGT-TokenReuseIp • TGT_ML_CoordinatedActivityMedium • TGT_ML_CoordinatedActivityHigh 	<p>Regeln wurden der Regelgruppe mit Aktion hinzugefügt. Count</p> <p>Die IP-Regel zur Wiederverwendung von Token erkennt und zählt die gemeinsame Nutzung von Token über IP-Adressen hinweg.</p> <p>Die Regeln für koordinierte Aktivitäten verwenden eine automatisierte Analyse des Webseitenverkehrs durch maschinelles Lernen (ML), um Aktivitäten im Zusammenhang mit Bots zu erkennen. In Ihrer Regelgruppenkonfiguration können Sie die Verwendung von ML deaktivieren. Mit dieser Version haben sich Kunden, die derzeit die angestrebte Schutzstufe verwenden, für die Verwendung von ML entschieden. Wenn Sie sich abmelden, werden die Regeln für koordinierte Aktivitäten deaktiviert.</p>	2023-09-06
AWS WAF Regelgruppe „Bot-Kontrolle“ <ul style="list-style-type: none"> • CategoryAI 	<p>Hinzufügung der Regel CategoryAI zur Regelgruppe.</p>	2023-08-30

Regelgruppe und Regeln	Beschreibung	Datum
Verwaltete Regelgruppe „Core Rule Set“ (CRS) <ul style="list-style-type: none"> • RestrictedExtensions_URI_PATH • RestrictedExtensions_QUERY_ARGUMENTS • EC2MetaDataSSRF_COOKIE • EC2MetaDataSSRF_QUERY_ARGUMENTS • EC2MetaDataSSRF_BODY • EC2MetaDataSSRF_URI_PATH 	<p>Die statische Version 1.7 dieser Regelgruppe wurde veröffentlicht.</p> <p>Eingeschränkte Erweiterungen und SSRF-Regeln für EC2-Metadaten wurden aktualisiert, um die Erkennung zu verbessern und Fehlalarme zu reduzieren.</p>	2023-07-26
AWS WAF Regelgruppe Betrugsprävention (ACFP) zur Kontoerstellung bei der Betrugsbekämpfung <p>Alle Regeln in neuer Regelgruppe</p>	Hinzufügung der Regelgruppe AWSManagedRulesACFPRuleSet .	2023-06-13

Regelgruppe und Regeln	Beschreibung	Datum
Verwaltete Regelgruppe „Linux Operating System“ <ul style="list-style-type: none"> • LFI_HEADER • LFI_URIPATH • LFI_QUERYSTRING 	<p>Die statische Version 2.2 dieser Regelgruppe wurde veröffentlicht.</p> <p>Signaturen wurden hinzugefügt, um die Erkennung zu verbessern.</p>	2023-05-22
Verwaltete Regelgruppe „Core Rule Set“ (CRS) <ul style="list-style-type: none"> • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH 	<p>Die statische Version 1.6 dieser Regelgruppe wurde veröffentlicht.</p> <p>Die Regeln für Cross-Site Scripting (XSS) und eingeschränkte Erweiterungen wurden aktualisiert, um die Erkennung zu verbessern und Fehlalarme zu reduzieren.</p>	2023-04-28

Regelgruppe und Regeln	Beschreibung	Datum
<p>Über PHP-Anwendung verwaltete Regelgruppe</p> <ul style="list-style-type: none"> • PHPHighRiskMethods Variables_BODY aktualisiert • Entfernt PHPHighRiskMethodsVariables_QUERYARGUMENTS • PHPHighRiskMethods Variables_QUERYSTRING hinzugefügt • PHPHighRiskMethods Variables_HEADER hinzugefügt 	<p>Die statische Version 2.0 dieser Regelgruppe wurde veröffentlicht.</p> <p>Signaturen wurden hinzugefügt, um die Erkennung in allen Regeln zu verbessern.</p> <p>Ersetzte die Regel PHPHighRiskMethods Variables_QUERYARGUMENTS durch PHPHighRiskMethods Variables_QUERYSTRING, die die gesamte Abfragezeichenfolge überprüft und nicht nur die Abfrageargumente.</p> <p>Die Regel wurde hinzugefügt PHPHighRiskMethods Variables_HEADER, um den Geltungsbereich auf alle Header auszudehnen.</p> <p>Die folgenden Bezeichnungen wurden aktualisiert, sodass sie der Standardkennzeichnung für AWS verwaltete Regeln entsprechen:</p> <ul style="list-style-type: none"> • Alter Name: PHPHighRiskMethodsVariables_BODY Neuer Name: PHPHighRiskMethods Variables_Body 	<p>2023-02-27</p>

Regelgruppe und Regeln	Beschreibung	Datum
	<ul style="list-style-type: none"> Alter Name: PHPHighRiskMethodsVariables_QUERYARGUMENTS Neuer Name: PHPHighRiskMethodsVariables_QueryString 	
<p>AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen (ATP) zur Betrugsbekämpfung</p> <ul style="list-style-type: none"> VolumetricIpFailedLoginResponseHigh VolumetricSessionFailedLoginResponseHigh 	<p>Es wurden Regeln zur Überprüfung von Login-Antworten zur Verwendung mit geschützten CloudFront Amazon-Distributionen hinzugefügt. Diese Regeln können neue Anmeldeversuche von IP-Adressen und Kundensitzungen blockieren, die in letzter Zeit zu viele fehlgeschlagene Anmeldeversuche verursacht haben.</p>	15.02.2023

Regelgruppe und Regeln	Beschreibung	Datum
Verwaltete Regelgruppe „Core Rule Set“ (CRS)	Die statische Version 1.5 dieser Regelgruppe wurde veröffentlicht.	2023-01-25
<ul style="list-style-type: none">• NoUserAgent_HEADER• CrossSiteScripting_COOKIE• CrossSiteScripting_QUERYARGUMENTS• CrossSiteScripting_BODY• CrossSiteScripting_URI_PATH	Die Cross Site Scripting (XSS) -Filter wurden aktualisiert, um die Erkennung zu verbessern.	

Regelgruppe und Regeln	Beschreibung	Datum
<p>Verwaltete Regelgruppe „Linux Operating System“</p> <ul style="list-style-type: none">• LFI_COOKIE - entfernt• LFI_HEADER - hinzugefügt• LFI_URIPATH• LFI_QUERYSTRING	<p>Statische Version 2.1 dieser Regelgruppe veröffentlicht.</p> <p>Die Regel LFI_COOKIE und ihre Bezeichnung <code>aws:waf:managed:aws:linux-os:LFI_Cookie</code> wurden entfernt und durch die neue Regel LFI_HEADER und ihre Bezeichnung <code>aws:waf:managed:aws:linux-os:LFI_Header</code> ersetzt. Durch diese Änderung wird die Prüfung auf mehrere Header ausgedehnt.</p> <p>Allen Regeln wurden Texttransformationen und Signaturen hinzugefügt, um die Erkennung zu verbessern.</p>	15.12.2022

Regelgruppe und Regeln	Beschreibung	Datum
Verwaltete Regelgruppe „Core Rule Set“ (CRS)	Die statische Version 1.4 dieser Regelgruppe wurde veröffentlicht.	05.12.2022
<ul style="list-style-type: none">• NoUserAgent_HEADER• CrossSiteScripting_COOKIE• CrossSiteScripting_QUERYARGUMENTS• CrossSiteScripting_BODY• CrossSiteScripting_URI_PATH	Es wurde eine Texttransformation hinzugefügt, NoUserAgent_HEADER um alle Null-Bytes zu entfernen. Die Filter in den Cross-Site-Scripting-Regeln wurden aktualisiert, um die Erkennung zu verbessern.	

Regelgruppe und Regeln	Beschreibung	Datum
<p>Verwaltete Regelgruppe „Known Bad Inputs“</p> <ul style="list-style-type: none"> • JavaDeserializatio nRCE_BODY • JavaDeserializatio nRCE_URIPATH • JavaDeserializatio nRCE_HEADER • JavaDeserializatio nRCE_QUERYSTRING • Host_localhost_HEA DER 	<p>Die statische Version 1.17 dieser Regelgruppe wurde veröffentlicht.</p> <p>Die Java-Deserialisierungsregeln wurden aktualisiert, um die Erkennung von Anfragen hinzuzufügen, die Apache CVE-2022-42889 entsprechen, einer Sicherheitslücke in Apache Commons Text vor 1.10.0, einer Sicherheitslücke in Apache Commons Text-Versionen vor 1.10.0. Weitere Informationen finden Sie unter NIST: National Vulnerability Database: CVE-2022-42889 Detail und CVE-2022-42889: Apache Commons Text vor 1.10.0 erlaubt RCE, wenn es aufgrund unsicherer Interpolationsstandards auf nicht vertrauenswürdige Eingaben angewendet wird.</p> <p>Verbesserte Erkennung in Host_localhost_HEA DER</p>	<p>20.10.2022</p>

Regelgruppe und Regeln	Beschreibung	Datum
<p>Verwaltete Regelgruppe „Known Bad Inputs“</p> <ul style="list-style-type: none"> • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URI_PATH • Log4JRCE_BODY 	<p>Die statische Version 1.16 dieser Regelgruppe wurde veröffentlicht.</p> <p>Fehlalarme, die in Version AWS 1.15 identifiziert wurden, wurden entfernt.</p>	05.10.2022
<p>Verwaltete Regelgruppe „POSIX Operating System“</p> <p>Über PHP-Anwendung verwaltete Regelgruppe</p> <p>WordPress Von der Anwendung verwaltete Regelgruppe</p>	Die dokumentierten Labelnamen wurden korrigiert.	19.09.2022
<p>IP-Reputationsregelgruppen</p> <ul style="list-style-type: none"> • AWSManagedIPDDoSList 	<p>Diese Änderung ändert nichts daran, wie die Regelgruppe mit dem Webverkehr umgeht.</p> <p>Laut Amazon Threat Intelligence wurde eine neue Regel hinzugefügt, mit Count der nach Angaben von Amazon Threat Intelligence nach IP-Adressen gesucht werden kann, die aktiv an DDoS-Aktivitäten beteiligt sind.</p>	30.08.2022

Regelgruppe und Regeln	Beschreibung	Datum
<p>Verwaltete Regelgruppe „Known Bad Inputs“</p> <ul style="list-style-type: none"> Log4JRCE Log4JRCE_HEADER Log4JRCE_QUERYSTRING Log4JRCE_URI_PATH Log4JRCE_BODY JavaDeserializationRCE_HEADER JavaDeserializationRCE_BODY JavaDeserializationRCE_URI_PATH JavaDeserializationRCE_QUERYSTRING Host_localhost_HEADER PROPFIND_METHOD 	<p>Die statische Version 1.15 dieser Regelgruppe wurde veröffentlicht.</p> <p>Es wurde entfernt Log4JRCE und durch Log4JRCE_HEADER „, und Log4JRCE_QUERYSTRING Log4JRCE_URI „, ersetzt Log4JRCE_BODY „, um Fehlalarme genauer zu überwachen und zu verwalten.</p> <p>Es wurden Signaturen hinzugefügt, um die Erkennung PROPFIND_METHOD und Blockierung aller JavaDeserializationRCE* Log4JRCE* Regeln zu verbessern.</p> <p>Die Bezeichnungen wurden aktualisiert, um die Groß- und Kleinschreibung in Host_localhost_HEADER und in allen JavaDeserializationRCE* Regeln zu korrigieren.</p> <p>Die Beschreibung von JavaDeserializationRCE_HEADER wurde korrigiert.</p>	22.08.2022

Regelgruppe und Regeln	Beschreibung	Datum
AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen (ATP) zur Betrugsbekämpfung <ul style="list-style-type: none"> UnsupportedCognito IDP 	Es wurde eine Regel hinzugefügt, um die Verwendung der verwalteten Regelgruppe zur Verhinderung von Kontoübernahmen für den Amazon Cognito Cognito-Benutzerpool-Webverkehr zu verhindern.	11.08.2022
Verwaltete Regelgruppe „Core Rule Set“ (CRS)	AWS hat ein geplantes Ablaufdatum für Versionen <code>Version_1.2</code> und für <code>Version_2.0</code> die Regelgruppe. Die Versionen laufen am 9. September 2022 ab. Informationen zum Ablauf der Version finden Sie unter Versionsverwaltung mit verwalteten Regelgruppen .	09.06.2022
Verwaltete Regelgruppe „Core Rule Set“ (CRS) <ul style="list-style-type: none"> GenericLFI_URIPATH GenericRFI_URIPATH 	Version 1.3 dieser Regelgruppe veröffentlicht. In dieser Version werden die Spielsignaturen in den Regeln aktualisiert <code>GenericLFI_URIPATH</code> und <code>GenericRFI_URIPATH</code> , um die Erkennung zu verbessern.	24.05.2022
AWS WAF Regelgruppe „Bot-Kontrolle“ <ul style="list-style-type: none"> CategoryEmailClient 	Hinzufügung der Regel <code>CategoryEmailClient</code> zur Regelgruppe.	06.04.2022

Regelgruppe und Regeln	Beschreibung	Datum
<p>Verwaltete Regelgruppe „Known Bad Inputs“</p> <ul style="list-style-type: none"> • JavaDeserializatio nRCE_HEADER • JavaDeserializatio nRCE_BODY • JavaDeserializatio nRCE_URI • JavaDeserializatio nRCE_QUERYSTRING 	<p>Veröffentlichung von Version 1.14 dieser Regelgruppe. Umstellung der vier JavaDeserializtion RCE -Regeln auf den Block-Modus.</p>	<p>31.03.2022</p>
<p>Verwaltete Regelgruppe „Known Bad Inputs“</p> <ul style="list-style-type: none"> • JavaDeserializatio nRCE_HEADER_RC_COU NT • JavaDeserializatio nRCE_BODY_RC_COUNT • JavaDeserializatio nRCE_URI_RC_COUNT • JavaDeserializatio nRCE_QUERYSTRING_R C_COUNT 	<p>Veröffentlichung von Version 1.13 dieser Regelgruppe. Aktualisierung der Texttransformation für Spring Core- und Cloud Function-RCE-Schwachstellen. Diese Regeln befinden sich im Zählmodus, um Metriken zu sammeln und übereinstimmende Muster auszuwerten. Die Kennzeichnung kann verwendet werden, um Anforderungen in einer benutzerdefinierten Regel zu blockieren. Eine nachfolgende Version wird mit diesen Regeln im Blockmodus bereitgestellt.</p>	<p>31.03.2022</p>

Regelgruppe und Regeln	Beschreibung	Datum
<p>Verwaltete Regelgruppe „Known Bad Inputs“</p> <ul style="list-style-type: none"> • JavaDeserializatio nRCE_HEADER_RC_COU NT • JavaDeserializatio nRCE_BODY_RC_COUNT • JavaDeserializatio nRCE_URI_RC_COUNT • JavaDeserializatio nRCE_QUERYSTRING_R C_COUNT • Log4JRCE_HEADER • Log4JRCE_QUERYSTRI NG • Log4JRCE_URI • Log4JRCE_BODY • Log4JRCE 	<p>Veröffentlichung von Version 1.12 dieser Regelgruppe. Hinzufügung von Signaturen für die Spring Core- und Cloud Function-RCE-Schwachstellen. Diese Regeln befinden sich im Zählmodus, um Metriken zu sammeln und übereinstimmende Muster auszuwerten. Die Kennzeichnung kann verwendet werden, um Anforderungen in einer benutzerdefinierten Regel zu blockieren. Eine nachfolgende Version wird mit diesen Regeln im Blockmodus bereitgestellt.</p> <p>Die RegelnLog4JRCE_HEADER , Log4JRCE_QUERYSTRING Log4JRCE_URI , und wurden entfernt Log4JRCE_BODY und durch die Regel ersetztLog4JRCE.</p>	30.03.2022
<p>IP-Reputationsregelgruppen</p> <ul style="list-style-type: none"> • AWSManagedReconnai ssanceList 	<p>AWSManagedReconnai ssanceList -Regel zum Ändern der Aktion von Block auf Count aktualisiert.</p>	15.02.2022

Regelgruppe und Regeln	Beschreibung	Datum
AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen (ATP) zur Betrugsbekämpfung Alle Regeln in neuer Regelgruppe	Hinzufügung der Regelgruppe AWSManagedRulesATP RuleSet .	11.02.2022
Verwaltete Regelgruppe „Known Bad Inputs“ <ul style="list-style-type: none"> • Log4JRCE • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URI • Log4JRCE_BODY 	Veröffentlichung von Version 1.9 dieser Regelgruppe. Entfernung der Regel Log4JRCE und Ersatz dieser Regel durch die Regeln Log4JRCE_HEADER , Log4JRCE_QUERYSTRING , Log4JRCE_URI und Log4JRCE_BODY , um die Flexibilität bei der Nutzung dieser Funktionalität zu gewährleisten. Hinzufügung von Signaturen, um die Erkennung und Blockierung zu verbessern.	28.01.2022

Regelgruppe und Regeln	Beschreibung	Datum
Core Rule Set (CRS) <ul style="list-style-type: none"> • CrossSiteScripting_URI_PATH • CrossSiteScripting_BODY • CrossSiteScripting_QUERY_ARGUMENTS • CrossSiteScripting_COOKIE 	Version 2.0 dieser Regelgruppe veröffentlicht. Für diese Regeln wurden Erkennungssignaturen optimiert, um Fehlalarme zu reduzieren. Ersetzung der URL_DECODE -Texttransformation durch die doppelte URL_DECODE_UNI -Texttransformation. Hinzufügung der HTML_ENTITY_DECODE -Texttransformation.	10.01.2022
Core Rule Set (CRS) <ul style="list-style-type: none"> • RestrictedExtensions_URI_PATH • RestrictedExtensions_QUERY_ARGUMENTS 	Im Rahmen der Veröffentlichung von Version 2.0 dieser Regelgruppe wurde die URL_DECODE_UNI Texttransformation hinzugefügt. Entfernung der URL_DECODE -Texttransformation aus RestrictedExtensions_URI_PATH .	10.01.2022

Regelgruppe und Regeln	Beschreibung	Datum
<p>SQL-Datenbank</p> <ul style="list-style-type: none"> • SQLi_BODY • SQLi_QUERYARGUMENTS • SQLi_COOKIE • SQLi_URI_PATH • SQLiExtendedPatterns_BODY • SQLiExtendedPatterns_QUERYARGUMENTS 	<p>Version 2.0 dieser Regelgruppe veröffentlicht. Ersetzung der URL_DECODE -Texttransformation durch die doppelte URL_DECODE_UNI -Texttransformation und Hinzufügung der COMPRESS_WHITE_SPACE -Texttransformation.</p> <p>Hinzufügung weiterer Erkennungssignaturen zu SQLiExtendedPatterns_QUERYARGUMENTS .</p> <p>Hinzufügung der JSON-Inspektion zu SQLi_BODY .</p> <p>Hinzufügung der Regel SQLiExtendedPatterns_BODY .</p> <p>Entfernung der Regel SQLi_URI_PATH .</p>	10.01.2022
<p>Known Bad Inputs</p> <ul style="list-style-type: none"> • Log4JRCE 	<p>Veröffentlichung von Version 1.8 der Regel Log4JRCE zur Verbesserung der Header-Inspektion und der Übereinstimmungskriterien.</p>	17.12.2021

Regelgruppe und Regeln	Beschreibung	Datum
Known Bad Inputs <ul style="list-style-type: none"> • Log4JRCE 	Veröffentlichung von Version 1.4 der Regel Log4JRCE zur Abstimmung der Übereinstimmungskriterien und zur Prüfung zusätzlicher Header. Veröffentlichung von Version 1.5 zur Abstimmung der Übereinstimmungskriterien.	11.12.2021
Known Bad Inputs <ul style="list-style-type: none"> • Log4JRCE • BadAuthToken_COOKIE_AUTHORIZATION 	Hinzufügung von Version 1.2 der Regel Log4JRCE als Reaktion auf das kürzlich bekanntgegebene Sicherheitsproblem in Log4j. Weitere Informationen finden Sie unter CVE-2021-44228 . Diese Regel prüft gängige URI-Pfade, Abfragezeichenfolgen, die ersten 8 KB des Anforderungstextes und gängige Header. Die Regel verwendet doppelte URL_DECODE_UNICODE-Texttransformationen. Veröffentlichung von Version 1.3 von Log4JRCE zur Abstimmung der Übereinstimmungskriterien und zur Prüfung zusätzlicher Header. Entfernung der Regel BadAuthToken_COOKIE_AUTHORIZATION .	10.12.2021

In der folgenden Tabelle sind die Änderungen aufgeführt, die vor Dezember 2021 vorgenommen wurden.

Regelgruppe und Regeln	Beschreibung	Datum	
Amazon IP Reputation List	AWSManagedReconnaissanceList	Hinzufügung der Regel AWSManagedReconnaissanceList im Überwachungs-/Zählmodus. Diese Regel enthält IP-Adressen, die Ressourcen ausspionieren. AWS	23.11.2021
Windows Operating System	WindowsShellCommands PowerShellCommands	Drei neue Regeln für WindowsShell Befehle hinzugefügt: WindowsShellCommands_COOKIE WindowsShellCommands_QUERYARGUMENTS , und WindowsShellCommands_BODY Eine neue PowerShell Regel wurde hinzugefügt: PowerShellCommands_COOKIE .	2021-11-23

Regelgruppe und Regeln	Beschreibung	Datum	
		<p>Umstrukturierung der PowerShell Comands - Regelbenennung durch Entfernen der Zeichenfolgen „_Set1“ und „_Set2“.</p> <p>Hinzufügung von umfassenderen Erkennungssignaturen zu PowerShell Rules .</p> <p>Hinzufügung der URL_DECODE_UNI - Texttransformation zu allen Regeln für das Windows-Betriebssystem.</p>	

Regelgruppe und Regeln	Beschreibung	Datum	
Linux Operating System	LFI_URIPATH LFI_QUERYSTRING LFI_BODY LFI_COOKIE	Doppelte URL_DECODE E Texttransformation durch Double ersetzt. URL_DECODE_UNI Hinzufügung von NORMALIZE _PATH_WIN als zweiter Texttrans formation. Ersetzung der LFI_BODY-Regel durch die LFI_COOKIE -Regel. Hinzufügung von umfassenderen Erkennungssignatur en für alle LFI- Regeln.	2021-11-23
Core Rule Set (CRS)	SizeRestrictions_BODY	Die Größenbeschränkung wurde reduziert, um Webanforderungen mit Textnutzlasten von mehr als 8 KB zu blockieren. Zuvor lag das Limit bei 10 KB.	27.10.2021

Regelgruppe und Regeln	Beschreibung	Datum	
Core Rule Set (CRS)	EC2MetaDa taSSRF_BODY EC2MetaDa taSSRF_COOKIE EC2MetaDa taSSRF_URI_PATH EC2MetaDa taSSRF_QUERY_ARGUMENTS	Hinzufügung weiterer Erkennungssignatur en. Hinzufügung der doppelten Unicode-U RL-Dekodierung zur Verbesserung des Blockierens.	27.10.2021
Core Rule Set (CRS)	GenericLF I_QUERY_ARGUMENTS GenericLF I_URI_PATH Restrict edExtensions_URI_PATH Restrict edExtensions_QUERY_ARGUMENTS	Hinzufügung der doppelten Unicode-U RL-Dekodierung zur Verbesserung des Blockierens.	27.10.2021

Regelgruppe und Regeln	Beschreibung	Datum	
Core Rule Set (CRS)	GenericRF I_QUERYAR GUMENTS GenericRFI_BODY GenericRF I_URIPATH	Aktualisierung der Regelsignaturen, um falsch positive Ergebnisse zu reduzieren (basierend auf Kundenfeedback). Hinzufügung der doppelten Unicode-URL-Dekodierung zur Verbesserung des Blockierens.	27.10.2021
Alle	Alle Regeln	Allen Regeln, die noch keine Kennzeichnung unterstützten, wurde Unterstützung für AWS WAF Labels hinzugefügt.	25.10.2021
Amazon IP Reputation List	AWSManagedIPReputationList_XXXX	Die IP-Reputationsliste wurde neu strukturiert, Suffixe aus dem Regelnamen entfernt und Unterstützung für Labels hinzugefügt. AWS WAF	04.05.2021
Anonymous IP List	AnonymousIPList HostingProviderList	Unterstützung für AWS WAF Labels hinzugefügt.	2021-05-04
Bot-Steuerung	Alle	Hinzufügung des Regelsatzes „Bot-Steuerung“.	01.04.2021

Regelgruppe und Regeln	Beschreibung	Datum	
Core Rule Set (CRS)	GenericRF I_QUERYAR GUMENTS	Hinzufügung der doppelten URL-Dekod ierung.	03.03.2021
Core Rule Set (CRS)	Restricte dExtensio ns_URIPATH	Verbesserung der Konfiguration der Regeln und Hinzufügu ng einer zusätzlichen URL-Dekodierung.	03.03.2021
Admin Protection	AdminProt ection_URIPATH	Hinzufügung der doppelten URL-Dekod ierung.	03.03.2021
Known Bad Inputs	ExploitablePaths_U RIPATH	Verbesserung der Konfiguration der Regeln und Hinzufügu ng einer zusätzlichen URL-Dekodierung.	03.03.2021
Linux Operating System	LFI_QUERY ARGUMENTS	Verbesserung der Konfiguration der Regeln und Hinzufügu ng einer zusätzlichen URL-Dekodierung.	03.03.2021
Windows Operating System	Alle	Verbesserung der Konfiguration der Regeln.	23.09.2020

Regelgruppe und Regeln	Beschreibung	Datum	
PHP-Anwendung	PHPHighRiskMethods Variables_QUERYARGUMENTS PHPHighRiskMethods Variables_BODY	Änderung der Texttransformation von HTML-Dekodierung in URL-Dekodierung, um Blockierung zu verbessern.	2020-09-16
POSIX-Betriebssystem	UNIXShell CommandsVariables_QUERYARGUMENTS UNIXShell CommandsVariables_BODY	Änderung der Texttransformation von HTML-Dekodierung in URL-Dekodierung, um Blockierung zu verbessern.	16.09.2020
Core Rule Set	GenericLFI_QUERYARGUMENTS GenericLFI_URI_PATH GenericLFI_BODY	Änderung der Texttransformation von HTML-Dekodierung in URL-Dekodierung, um Blockierung zu verbessern.	2020-08-07

Regelgruppe und Regeln	Beschreibung	Datum	
Linux Operating System	LFI_URIPATH LFI_QUERY LFI_ARGUMENTS LFI_BODY	Änderung der Texttransformation von HTML-Entitätsdekodierung in URL-Dekodierung, um Erkennung und Blockierung zu verbessern.	2020-05-19
Anonyme IP-Liste	Alle	Neue Regelgruppe blockiert Anfragen von Diensten IP-Reputationsregelgruppen , die die Verschleierung der Zuschaueridentität ermöglichen, um Bots und die Umgehung geografischer Beschränkungen zu verhindern.	2020-03-06
WordPress Bewerbung	WordPress ExploitableCommand s_QUERYSTRING	Neue Regel, die nach ausnutzbaren Befehlen in der Abfragezeichenfolge sucht.	2020-03-03

Regelgruppe und Regeln	Beschreibung	Datum	
Core Rule Set (CRS)	SizeRestrictions_QUERYSTRING SizeRestrictions_COOKIE_HEADER SizeRestrictions_BODY SizeRestrictions_URI_PATH	Die Größenschränkungen wurden angepasst, um die Genauigkeit zu verbessern.	2020-03-03
SQL-Datenbank	SQLi_URI_PATH	Die Regeln überprüfen jetzt den Nachrichten-URI.	2020-01-23
SQL-Datenbank	SQLi_BODY SQLi_QUERY_ARGUMENTS SQLi_COOKIE	Aktualisierte Texttransformationen.	2019-12-20

Regelgruppe und Regeln	Beschreibung	Datum	
Core Rule Set (CRS)	CrossSite Scripting _URIPATH	Aktualisierte Texttransformationen.	20.12.2019
	CrossSite Scripting_BODY		
	CrossSite Scripting _QUERYARGUMENTS		
	CrossSite Scripting _COOKIE		

AWS Marketplace verwaltete Regelgruppen

AWS Marketplace verwaltete Regelgruppen sind als Abonnement über die AWS Marketplace Konsole unter verfügbar [AWS Marketplace](#). Nachdem Sie eine AWS Marketplace verwaltete Regelgruppe abonniert haben, können Sie sie in verwenden AWS WAF. Um eine AWS Marketplace Regelgruppe in einer AWS Firewall Manager AWS WAF Richtlinie verwenden zu können, muss jedes Konto in Ihrer Organisation sie abonnieren.

Testen und optimieren Sie alle Änderungen an Ihren AWS WAF Schutzmaßnahmen, bevor Sie sie für den produktiven Datenverkehr verwenden. Weitere Informationen finden Sie unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

AWS Marketplace Preisgestaltung für Regelgruppen

AWS Marketplace Regelgruppen sind ohne langfristige Verträge und ohne Mindestverpflichtungen erhältlich. Wenn Sie eine Regelgruppe abonnieren, werden Ihnen monatliche Gebühren (auf Stunden umgelegt) und kontinuierliche Gebühren für Anforderungen nach Volumen berechnet. Weitere Informationen finden Sie unter [AWS WAF Preise](#) und in der Beschreibung der einzelnen AWS Marketplace Regelgruppen unter [AWS Marketplace](#).

Haben Sie Fragen zu einer AWS Marketplace Regelgruppe?

Wenn Sie Fragen zu einer Regelgruppe haben, die von einem AWS Marketplace Verkäufer verwaltet wird, und wenn Sie Änderungen an der Funktionalität beantragen möchten, wenden Sie sich an den Kundensupport des Anbieters. Kontaktinformationen finden Sie im Angebot des Anbieters unter [AWS Marketplace](#).

Der AWS Marketplace Regelgruppenanbieter legt fest, wie die Regelgruppe verwaltet wird, z. B. wie die Regelgruppe aktualisiert wird und ob die Regelgruppe versioniert ist. Der Anbieter bestimmt auch die Details der Regelgruppe, einschließlich der Regeln, Regelaktionen und aller Bezeichnungen, die die Regeln passenden Webanfragen hinzufügen.

AWS Marketplace Verwaltete Regelgruppen abonnieren

Sie können AWS Marketplace Regelgruppen auf der AWS WAF Konsole abonnieren und abbestellen.

Important

Um eine AWS Marketplace Regelgruppe in einer AWS Firewall Manager Richtlinie zu verwenden, muss jedes Konto in Ihrer Organisation zuerst diese Regelgruppe abonnieren.

Um eine AWS Marketplace verwaltete Regelgruppe zu abonnieren


1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich AWS Marketplace aus.
3. Wählen Sie im Abschnitt Available marketplace products den Namen einer Regelgruppe aus, um die Details und Preisinformationen anzuzeigen.
4. Wenn Sie die Regelgruppe abonnieren möchten, wählen Sie Continue.

Note

Wenn Sie diese Regelgruppe nicht abonnieren möchten, schließen Sie einfach diese Seite in Ihrem Browser.

5. Wählen Sie Set up your account.

6. Fügen Sie die Regelgruppe zu einer Web-ACL hinzu, ähnlich wie Sie eine individuelle Regel hinzufügen. Weitere Informationen finden Sie unter [Erstellen einer Web-ACL](#) oder [Bearbeiten einer Web-ACL](#).


 Note

Wenn Sie eine Regelgruppe zu einer Web-ACL hinzufügen, können Sie die Aktionen der Regeln in der Regelgruppe und des Ergebnisses der Regelgruppe überschreiben. Weitere Informationen finden Sie unter [Aktionsüberschreibungen in Regelgruppen](#).

Nachdem Sie eine AWS Marketplace Regelgruppe abonniert haben, verwenden Sie sie in Ihren Web-ACLs wie andere verwaltete Regelgruppen. Weitere Informationen finden Sie unter [Erstellen einer Web-ACL](#).

Abbestellen von verwalteten Regelgruppen AWS Marketplace

Sie können sich auf AWS Marketplace der Konsole von Regelgruppen abmelden. AWS WAF

 Important

Um die Abonnementgebühren für eine AWS Marketplace verwaltete Regelgruppe zu beenden, müssen Sie sie aus allen Web-ACLs in AWS WAF und in allen Firewall Manager AWS WAF Manager-Richtlinien entfernen und sich zusätzlich von ihr abmelden. Wenn Sie sich von einer AWS Marketplace verwalteten Regelgruppe abmelden, sie aber nicht aus Ihren Web-ACLs entfernen, wird Ihnen das Abonnement weiterhin in Rechnung gestellt.

Um sich von einer AWS Marketplace verwalteten Regelgruppe abzumelden

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Entfernen Sie die Regelgruppe aus allen Web-ACLs. Weitere Informationen finden Sie unter [Bearbeiten einer Web-ACL](#).
3. Wählen Sie im Navigationsbereich AWS Marketplace aus.
4. Wählen Sie Manage Your Subscriptions.
5. Wählen Sie Cancel subscription neben den Namen der Regelgruppe, die Sie kündigen möchten.

6. Wählen Sie Yes, cancel subscription.

Problembehandlung bei AWS Marketplace Regelgruppen

Wenn Sie feststellen, dass eine AWS Marketplace Regelgruppe legitimen Datenverkehr blockiert, können Sie das Problem beheben, indem Sie die folgenden Schritte ausführen.

So behandeln Sie Probleme mit einer AWS Marketplace -Regelgruppe

1. Überschreiben Sie die Aktionen, um die Regeln zu zählen, die legitimen Datenverkehr blockieren. Sie können anhand der AWS WAF gesampelten Anfragen oder anhand von AWS WAF Protokollen feststellen, welche Regeln bestimmte Anfragen blockieren. Sie können die Regeln identifizieren, indem Sie sich das Feld `ruleGroupId` im Protokoll oder das Feld `RuleWithinRuleGroup` in der Stichprobenanforderung ansehen. Sie können die Regel im Muster `<Seller Name>#<RuleGroup Name>#<Rule Name>` identifizieren.
2. Wenn das Problem nicht gelöst wird, indem Sie bestimmte Regeln so einrichten, dass nur Anfragen gezählt werden, können Sie alle Regelaktionen überschreiben oder die Aktion für die AWS Marketplace Regelgruppe selbst von Keine Überschreibung auf Überschreiben ändern, um zu zählen. Dadurch kann die Webanforderung unabhängig von den einzelnen Regelaktionen innerhalb der Regelgruppe durchlaufen werden.
3. Nachdem Sie entweder die einzelne Regelaktion oder die gesamte AWS Marketplace Regelgruppenaktion außer Kraft gesetzt haben, wenden Sie sich an das Kundendienstteam des Regelgruppenanbieters, um das Problem weiter zu beheben. Kontaktinformationen finden Sie in der Regelgruppenliste auf den Produktlistenseiten auf AWS Marketplace.

Den Support kontaktieren AWS

Bei Problemen mit AWS WAF oder einer Regelgruppe, die von verwaltet wird AWS, wenden Sie sich an AWS Support. Bei Problemen mit einer Regelgruppe, die von einem AWS Marketplace Verkäufer verwaltet wird, wenden Sie sich an den Kundensupport des Anbieters. Kontaktinformationen finden Sie im Angebot des Anbieters unter AWS Marketplace.

Verwaltung Ihrer eigenen Regelgruppen

Sie können eine eigene Regelgruppe erstellen, um Regelsammlungen wiederzuverwenden, die Sie entweder nicht in den verwalteten Regelgruppenangeboten finden oder die Sie lieber selbst bearbeiten.

Erstellte Regelgruppen umfassen wie eine Web-ACL Regeln. Sie fügen Regeln zu einer Regelgruppe hinzu, wie Sie es von einer Web-ACL gewohnt sind. Wenn Sie eine eigene Regelgruppe anlegen, müssen Sie dafür eine unveränderliche Kapazitätsgrenze festlegen.

Themen

- [Erstellen einer Regelgruppe](#)
- [Regelgruppe bearbeiten](#)
- [Verwenden Ihrer Regelgruppe in einer Web-ACL](#)
- [Eine Regelgruppe mit einem anderen Konto teilen](#)
- [Löschen einer Regelgruppe](#)

Erstellen einer Regelgruppe

So erstellen Sie eine Regelgruppe

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich Rule groups (Regelgruppen) und dann Create rule group (Regelgruppe erstellen).
3. Geben Sie einen Namen und eine Beschreibung für die Regelgruppe ein. Sie verwenden diese, um den Regelsatz zu identifizieren, um ihn zu verwalten und zu verwenden.

Verwenden Sie keine Namen, die mit `AWS`, `ShieldPreFM`, oder `beginnenPostFM` beginnen. Diese Zeichenfolgen sind entweder reserviert oder könnten zu Verwechslungen mit Regelgruppen führen, die von anderen Diensten für Sie verwaltet werden. Siehe [Regelgruppen, die von anderen Services bereitgestellt werden](#).

Note

Sie können den Namen nach dem Anlegen der Regelgruppe nicht mehr ändern.

4. Wählen Sie unter Region die Region, in der Sie die Regelgruppe speichern möchten. Um eine Regelgruppe in Web-ACLs zu verwenden, die CloudFront Amazon-Distributionen schützen, müssen Sie die globale Einstellung verwenden. Sie können die globale Einstellung auch für regionale Anwendungen verwenden.
5. Wählen Sie Weiter aus.

6. Fügen Sie mit dem Rule-Builder-Assistenten Regeln zur Regelgruppe hinzu, wie Sie es auch bei der Verwaltung von Web-ACLs tun. Der einzige Unterschied besteht darin, dass Sie eine Regelgruppe nicht zu einer anderen Regelgruppe hinzufügen können.
7. Legen Sie für Capacity (Kapazität) die Grenze für die Verwendung von Web-ACL-Kapazitätseinheiten (Web ACL Capacity Units, WCUs) durch die Regelgruppe fest. Dies ist eine unveränderliche Einstellung. Informationen zu den WCUs finden Sie unter [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#).

Wenn Sie Regeln zur Regelgruppe hinzufügen, zeigt der Bereich Add rules and set capacity (Regeln hinzufügen und Kapazität festlegen) die minimal erforderliche Kapazität an. Diese basiert auf den Regeln, die Sie bereits hinzugefügt haben. Sie können diese und Ihre zukünftigen Pläne für die Regelgruppe verwenden, um die Kapazität abzuschätzen, die die Regelgruppe benötigt.

8. Überprüfen Sie die Einstellungen für die Regelgruppe und wählen Sie Create (Erstellen).

Regelgruppe bearbeiten

Um Regeln zu einer Regelgruppe hinzuzufügen oder zu entfernen oder Konfigurationseinstellungen zu ändern, greifen Sie mit dem Verfahren auf dieser Seite auf die Regelgruppe zu.

Risiken rund um Produktionsdatenverkehr

Wenn Sie eine Regelgruppe ändern, die Sie derzeit in einer Web-ACL verwenden, wirken sich diese Änderungen auf Ihr Web-ACL-Verhalten aus, unabhängig davon, wo sie verwendet wird. Testen und optimieren Sie alle Änderungen in einer Staging- oder Testumgebung, bis Sie mit den möglichen Auswirkungen auf Ihren Traffic zufrieden sind. Testen und optimieren Sie dann Ihre aktualisierten Regeln im Zählmodus mit Ihrem Produktionsdatenverkehr, bevor Sie sie aktivieren. Anleitungen finden Sie unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

Um eine Regelgruppe zu bearbeiten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich Rule groups (Regelgruppen).

3. Wählen Sie den Namen der Regelgruppe, die Sie bearbeiten möchten. Die Konsole leitet Sie zur Seite der Regelgruppe weiter.
4. Bearbeiten Sie die Regelgruppe nach Bedarf. Sie können die veränderbaren Eigenschaften der Regelgruppe bearbeiten, ähnlich wie Sie es bei der Erstellung getan haben. Die Konsole speichert Ihre Änderungen während Sie arbeiten.

Note

Wenn Sie den Namen einer Regel ändern und möchten, dass der Metrikname der Regel die Änderung widerspiegelt, müssen Sie auch den Metriknamen aktualisieren. AWS WAF aktualisiert den Metriknamen für eine Regel nicht automatisch, wenn Sie den Regelnamen ändern. Sie können den Metriknamen ändern, wenn Sie die Regel in der Konsole bearbeiten, indem Sie den JSON-Editor für Regeln verwenden. Sie können beide Namen auch über die APIs und in jeder JSON-Liste ändern, die Sie zur Definition Ihrer Web-ACL oder Regelgruppe verwenden.

Temporäre Inkonsistenzen bei Aktualisierungen

Wenn Sie eine Web-ACL oder andere AWS WAF Ressourcen erstellen oder ändern, dauert es wenig Zeit, bis die Änderungen in allen Bereichen, in denen die Ressourcen gespeichert sind, übernommen werden. Die Übertragungszeit kann zwischen einigen Sekunden und mehreren Minuten liegen.

Im Folgenden finden Sie Beispiele für temporäre Inkonsistenzen, die Ihnen bei der Übertragung von Änderungen möglicherweise auffallen:

- Wenn Sie nach der Erstellung einer Web-ACL versuchen, sie einer Ressource zuzuordnen, wird möglicherweise eine Ausnahme angezeigt, die darauf hinweist, dass die Web-ACL nicht verfügbar ist.
- Nachdem Sie einer Web-ACL eine Regelgruppe hinzugefügt haben, gelten die neuen Regelgruppenregeln möglicherweise in einem Bereich, in dem die Web-ACL verwendet wird, und nicht in einem anderen.
- Nachdem Sie eine Regelaktionseinstellung geändert haben, sehen Sie möglicherweise an einigen Stellen die alte Aktion und an anderen die neue Aktion.
- Nachdem Sie einem IP-Set, das in einer Sperrregel verwendet wird, eine IP-Adresse hinzugefügt haben, wird die neue Adresse möglicherweise in einem Bereich blockiert, während sie in einem anderen weiterhin zulässig ist.

Verwenden Ihrer Regelgruppe in einer Web-ACL

Um eine Regelgruppe in einer Web-ACL zu verwenden, fügen Sie sie der Web-ACL in einer Regelgruppen-Referenzanweisung hinzu.

Risiken rund um Produktionsdatenverkehr

Bevor Sie Änderungen an Ihrer Web-ACL für den Produktionsdatenverkehr implementieren, testen und optimieren Sie sie in einer Staging- oder Testumgebung, bis Sie mit den möglichen Auswirkungen auf Ihren Datenverkehr zufrieden sind. Testen und optimieren Sie anschließend Ihre aktualisierten Regeln im Zählmodus mit Ihrem Produktionsdatenverkehr, bevor Sie sie aktivieren. Anleitungen finden Sie unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

Note

Bei der Verwendung von mehr als 1.500 WCUs in einer Web-ACL fallen Kosten an, die über den Grundpreis für Web-ACL hinausgehen. Weitere Informationen finden Sie unter [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#) und [Preise zu AWS WAF](#).

Wenn Sie in der Konsole Regeln in Ihrer Web-ACL hinzufügen oder aktualisieren, wählen Sie auf der Seite Regeln und Regelgruppen hinzufügen die Option Regeln hinzufügen und dann Meine eigenen Regeln und Regelgruppen hinzufügen aus. Wählen Sie dann Rule group (Regelgruppe) und wählen Sie Ihre Regelgruppe aus der Liste aus.

In Ihrer Web-ACL können Sie das Verhalten einer Regelgruppe und ihrer Regeln ändern, indem Sie die einzelnen Regelaktionen auf Count oder eine andere Aktion festlegen. Dies kann Ihnen verschiedene Aufgaben erleichtern, etwa das Testen einer Regelgruppe, das Erkennen von falsch positiven Ergebnissen anhand von Regeln in einer Regelgruppe und das Anpassen der Behandlung Ihrer Anforderungen durch eine verwaltete Regelgruppe. Weitere Informationen finden Sie unter [Aktionsüberschreibungen in Regelgruppen](#).

Wenn Ihre Regelgruppe eine ratenbasierte Anweisung enthält, verfügt jede Web-ACL, in der Sie die Regelgruppe verwenden, über eine eigene Ratenverfolgung und -verwaltung für die ratenbasierte Regel – unabhängig von anderen Web-ACLs, in der Sie die Regelgruppe möglicherweise verwenden. Weitere Informationen finden Sie unter [Ratenbasierte Regelanweisung](#).

Temporäre Inkonsistenzen bei Updates

Wenn Sie eine Web-ACL oder andere AWS WAF Ressourcen erstellen oder ändern, dauert es wenig Zeit, bis die Änderungen in allen Bereichen, in denen die Ressourcen gespeichert sind, übernommen werden. Die Übertragungszeit kann zwischen einigen Sekunden und mehreren Minuten liegen.

Im Folgenden finden Sie Beispiele für temporäre Inkonsistenzen, die Ihnen bei der Übertragung von Änderungen möglicherweise auffallen:

- Wenn Sie nach der Erstellung einer Web-ACL versuchen, sie einer Ressource zuzuordnen, wird möglicherweise eine Ausnahme angezeigt, die darauf hinweist, dass die Web-ACL nicht verfügbar ist.
- Nachdem Sie einer Web-ACL eine Regelgruppe hinzugefügt haben, gelten die neuen Regelgruppenregeln möglicherweise in einem Bereich, in dem die Web-ACL verwendet wird, und nicht in einem anderen.
- Nachdem Sie eine Regelaktionseinstellung geändert haben, sehen Sie möglicherweise an einigen Stellen die alte Aktion und an anderen die neue Aktion.
- Nachdem Sie einem IP-Set, das in einer Sperrregel verwendet wird, eine IP-Adresse hinzugefügt haben, wird die neue Adresse möglicherweise in einem Bereich blockiert, während sie in einem anderen weiterhin zulässig ist.

Eine Regelgruppe mit einem anderen Konto teilen

Sie können eine Regelgruppe, die Sie besitzen, mit einem anderen AWS Konto teilen, damit sie von diesem Konto verwendet werden kann. Sie können dies nur über die AWS WAF API tun. Weitere Informationen finden Sie [PutPermissionPolicy](#) in der AWS WAF API-Referenz.

Löschen einer Regelgruppe

Befolgen Sie die Anweisungen in diesem Abschnitt, um eine Regelgruppe zu löschen.

Löschen von referenzierten Sets oder Regelgruppen

Wenn Sie eine Entität löschen, die Sie in einer Web-ACL verwenden können, z. B. einen IP-Satz, einen Regex-Mustersatz oder eine Regelgruppe, wird AWS WAF überprüft, ob die Entität derzeit in einer Web-ACL verwendet wird. Wenn es feststellt, dass es verwendet wird, werden Sie AWS WAF gewarnt. AWS WAF kann fast immer feststellen, ob eine Web-ACL auf eine Entität verweist. In seltenen Fällen ist dies jedoch nicht möglich. Wenn Sie sicherstellen müssen, dass die Entität derzeit

nicht verwendet, überprüfen Sie sie in den Web-ACLs, bevor Sie sie löschen. Wenn es sich bei der Entität um ein referenziertes Set handelt, stellen Sie sicher, dass keine Regelgruppen es verwenden.

So löschen Sie eine Regelgruppe

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich Rule groups (Regelgruppen).
3. Wählen Sie die Regelgruppe, die Sie löschen möchten. Wählen Sie dann Delete (Löschen).

Regelgruppen, die von anderen Services bereitgestellt werden

Wenn Sie oder ein Administrator in Ihrer Organisation den Ressourcenschutz verwenden AWS Firewall Manager oder AWS Shield Advanced verwalten AWS WAF, werden Ihnen möglicherweise Regelgruppen-Referenzanweisungen zu Web-ACLs in Ihrem Konto hinzugefügt.

Die Namen dieser Regelgruppen beginnen mit den folgenden Zeichenfolgen:

- **ShieldMitigationRuleGroup**— Diese Regelgruppen werden von geschützten Ressourcen der Anwendungsebene (Schicht 7) verwaltet AWS Shield Advanced und zur automatischen Abwehr von DDoS-Angriffen auf Anwendungsebene (Schicht 7) verwendet.

Wenn Sie die automatische DDoS-Abwehr auf Anwendungsebene für eine geschützte Ressource aktivieren, fügt Shield Advanced der Web-ACL, die Sie der Ressource zugeordnet haben, eine dieser Regelgruppen hinzu. Shield Advanced weist der Regelgruppen-Referenzanweisung eine Prioritätseinstellung von 10.000.000 zu, sodass sie nach den Regeln ausgeführt wird, die Sie in der Web-ACL konfiguriert haben. Weitere Informationen zu diesen Regelgruppen finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#).

Warning

Versuchen Sie nicht, diese Regelgruppe in Ihrer Web-ACL manuell zu verwalten. Löschen Sie insbesondere die `ShieldMitigationRuleGroup` Regelgruppen-Referenzanweisung nicht manuell aus Ihrer Web-ACL. Dies könnte unbeabsichtigte Folgen für alle Ressourcen haben, die mit der Web-ACL verknüpft sind. Verwenden Sie stattdessen Shield Advanced, um die automatischen Abwehrmaßnahmen der Ressourcen zu deaktivieren, die mit der

Web-ACL verknüpft sind. Shield Advanced entfernt die Regelgruppe für Sie, wenn sie für die automatische Schadensbegrenzung nicht benötigt wird.

- **PREFManaged** und **POSTFManaged** — Diese Regelgruppen werden verwaltet von AWS Firewall Manager. Firewall Manager stellt sie in Web-ACLs bereit, die Firewall Manager erstellt und verwaltet. Die Namen der Web-ACLs beginnen mit `FManagedWebACLV2`. Informationen zu diesen Web-ACLs und Regelgruppen finden Sie unter [AWS WAF Richtlinien](#).

AWS WAF Regeln

Eine AWS WAF Regel definiert, wie HTTP (S) -Webanfragen geprüft werden und welche Aktion bei einer Anfrage zu ergreifen ist, wenn sie den Inspektionskriterien entspricht. Sie definieren Regeln nur im Kontext einer Regelgruppe oder Web-ACL.

Regeln existieren nicht für AWS WAF sich allein. Sie sind keine AWS Ressourcen und sie haben keine Amazon-Ressourcennamen (ARNs). Sie können über den Namen in der Regelgruppe oder die Web-ACL, in der sie definiert ist, auf eine Regel zugreifen. Sie können Regeln verwalten und sie in andere Web-ACLs kopieren, indem Sie die JSON-Ansicht der Regelgruppe oder Web-ACL verwenden, die die Regel enthält. Sie können sie auch über den AWS WAF Console Rule Builder verwalten, der für Web-ACLs und Regelgruppen verfügbar ist.

Regelname

Jede Regel benötigt einen Namen. Vermeiden Sie Namen, die mit Regelgruppen oder Regeln beginnen, die für Sie von anderen Diensten verwaltet werden, AWS und Namen, die für Sie verwendet werden. Siehe [Regelgruppen, die von anderen Services bereitgestellt werden](#).

Note

Wenn Sie den Namen einer Regel ändern und möchten, dass der Metrikname der Regel die Änderung widerspiegelt, müssen Sie auch den Metriknamen aktualisieren. AWS WAF aktualisiert den Metriknamen für eine Regel nicht automatisch, wenn Sie den Regelnamen ändern. Sie können den Metriknamen ändern, wenn Sie die Regel in der Konsole bearbeiten, indem Sie den JSON-Editor für Regeln verwenden. Sie können beide Namen auch über die APIs und in jeder JSON-Liste ändern, mit der Sie Ihre Web-ACL oder Regelgruppe definieren.

Erklärung zur Regel

Jede Regel erfordert außerdem eine Regelaussage, die definiert, wie die Regel Webanfragen prüft. Die Regelanweisung kann je nach Regel und Anweisungstyp weitere, verschachtelte Anweisungen in beliebiger Tiefe enthalten. Einige Regelaussagen basieren auf einer Reihe von Kriterien. Sie können beispielsweise bis zu 10.000 IP-Adressen oder IP-Adressbereiche für eine IP-Set-Übereinstimmungsregel angeben.

Sie können Regeln definieren, die nach Kriterien wie den folgenden suchen:

- Skripts sind möglicherweise bösartig. Angreifer betten Skripts ein, die Sicherheitslücken in Webanwendungen ausnutzen. Dies wird als Cross-Site-Scripting (XSS) bezeichnet.
- IP-Adressen oder Adressbereiche, aus denen Anforderungen stammen.
- Land oder geografischer Standort, von dem die Anforderung stammt.
- Länge eines angegebenen Teils der Anforderung, z. B. die Abfragezeichenfolge.
- SQL-Code, der möglicherweise bösartig ist. Angreifer, die versuchen, Daten aus Ihrer Datenbank zu extrahieren, indem sie bösartigen SQL-Code in eine Webanforderung einbetten. Dies wird als SQL Injection bezeichnet.
- Zeichenfolgen, die in der Anforderung angezeigt werden, z. B. Werte im User-Agent-Header oder Textzeichenfolgen in der Abfragezeichenfolge. Sie können auch reguläre Ausdrücke (Regex) verwenden, um diese Zeichenfolgen anzugeben.
- Bezeichnungen, die vorherige Regeln in der Web-ACL der Anforderung hinzugefügt haben.

Zusätzlich zu Anweisungen mit Prüfkriterien für Webanfragen, wie die in der obigen Liste, werden logische Anweisungen für AND, und AWS WAF unterstützt OR, NOT die Sie verwenden, um Anweisungen in einer Regel zu kombinieren.

Basierend auf aktuellen Anforderungen, die Sie von einem Angreifer erhalten haben, können Sie beispielsweise eine ratenbasierte Regel mit einer verschachtelten AND-Regelanweisung erstellen, die die folgenden verschachtelten Anweisungen kombiniert:

- Die Anforderungen stammen von 192.0.2.44.
- Sie enthalten den Wert BadBot im User-Agent-Header.
- Sie scheinen schädlichen SQL-ähnlichen Code in die Abfragezeichenfolge einzufügen.

In diesem Fall muss die Webanforderung mit allen Anweisungen übereinstimmen, damit die oberste AND-Anweisung übereinstimmt.

Themen

- [Regelaktion](#)
- [Grundlagen der Regelerklärung](#)
- [Statements der Match-Regel](#)
- [Logische Regelaussagen](#)
- [Ratenbasierte Regelanweisung](#)
- [Regelgruppenregelanweisungen](#)

Regelaktion

Die Regelaktion legt fest, AWS WAF was mit einer Webanfrage geschehen soll, wenn sie den in der Regel definierten Kriterien entspricht. Sie können jeder Regelaktion optional ein benutzerdefiniertes Verhalten hinzufügen.

Note

Regelaktionen können beendend oder nicht beendend sein. Eine abschließende Aktion stoppt die Web-ACL-Auswertung der Anfrage und lässt sie entweder an Ihre geschützte Anwendung weiterleiten oder blockiert sie.

Hier sind die Optionen für die Regelaktion:

- **Allow**— AWS WAF ermöglicht die Weiterleitung der Anfrage zur Bearbeitung und Beantwortung an die geschützte AWS Ressource. Dies ist eine abschließende Aktion. In von Ihnen definierten Regeln können Sie benutzerdefinierte Header in die Anfrage einfügen, bevor Sie sie an die geschützte Ressource weiterleiten.
- **Block**— AWS WAF blockiert die Anfrage. Dies ist eine abschließende Aktion. Standardmäßig antwortet Ihre geschützte AWS Ressource mit einem 403 (Forbidden) HTTP-Statuscode. In Regeln, die Sie definieren, können Sie die Antwort anpassen. Wenn eine Anfrage AWS WAF blockiert wird, bestimmen die Block Aktionseinstellungen die Antwort, die die geschützte Ressource an den Client zurücksendet.

- **Count**— AWS WAF zählt die Anfrage, bestimmt aber nicht, ob sie zugelassen oder blockiert werden soll. Dies ist eine Aktion, die nicht beendet wird. AWS WAF setzt die Verarbeitung der verbleibenden Regeln in der Web-ACL fort. In von Ihnen definierten Regeln können Sie benutzerdefinierte Header in die Anforderung einfügen und Labels hinzufügen, mit denen andere Regeln übereinstimmen können.
- **CAPTCHA und Challenge** — AWS WAF verwendet CAPTCHA-Rätsel und stille Challenges, um zu überprüfen, ob die Anfrage nicht von einem Bot stammt, und AWS WAF verwendet Tokens, um die letzten erfolgreichen Kundenantworten nachzuverfolgen.

Note

Ihnen werden zusätzliche Gebühren berechnet, wenn Sie die Aktion CAPTCHA oder die Challenge Regel in einer Ihrer Regeln oder als Überschreibung von Regelaktionen in einer Regelgruppe verwenden. Weitere Informationen finden Sie unter [AWS WAF - Preisgestaltung](#).

Diese Regelaktionen können abhängig vom Status des Tokens in der Anfrage beendet oder nicht beendet werden:

- **Nicht terminierend für ein gültiges, nicht abgelaufenes Token** — Wenn das Token gemäß dem konfigurierten CAPTCHA oder der Challenge-Immunitätszeit gültig und nicht abgelaufen ist, wird die Anfrage ähnlich wie die Aktion behandelt. AWS WAF Count AWS WAF überprüft die Webanforderung weiterhin auf der Grundlage der verbleibenden Regeln in der Web-ACL. Ähnlich wie bei der Count Konfiguration können Sie in Regeln, die Sie definieren, diese Aktionen optional mit benutzerdefinierten Headern konfigurieren, die in die Anfrage eingefügt werden, und Sie können Labels hinzufügen, mit denen andere Regeln übereinstimmen können.
- **Beenden mit blockierter Anfrage für ein ungültiges oder abgelaufenes Token** — Wenn das Token ungültig ist oder der angegebene Zeitstempel abgelaufen ist, wird die Überprüfung der Webanforderung AWS WAF beendet und die Anfrage blockiert, ähnlich wie bei der Aktion. Block AWS WAF antwortet dem Client dann mit einem benutzerdefinierten Antwortcode. Denn CAPTCHA wenn der Inhalt der Anfrage darauf hindeutet, dass der Client-Browser damit umgehen kann, AWS WAF sendet er ein CAPTCHA-Puzzle in einem JavaScript Interstitial, das menschliche Kunden von Bots unterscheiden soll. Für die Challenge Aktion wird ein JavaScript Interstitial mit einer stillen Aufforderung AWS WAF gesendet, mit der normale Browser von Sitzungen unterschieden werden sollen, die von Bots ausgeführt werden.

Weitere Informationen finden Sie unter [CAPTCHA und Challenge in AWS WAF](#).

Informationen zum Anpassen von Anforderungen und Antworten finden Sie unter [Benutzerdefinierte Webanforderungen und Antworten in AWS WAF](#).

Informationen zum Hinzufügen von Bezeichnungen zu übereinstimmenden Anforderungen finden Sie unter [AWS WAF Labels auf Webanfragen](#).

Informationen zur Interaktion zwischen Web-ACL und Regeleinstellungen finden Sie unter [Auswertung von Web-ACL-Regeln und -Regelgruppen](#)

Grundlagen der Regelerklärung

Regelanweisungen sind der Teil einer Regel, der festlegt, AWS WAF wie eine Webanfrage untersucht wird. Wenn AWS WAF die Prüfkriterien in einer Webanfrage gefunden werden, sagen wir, dass die Webanforderung mit der Anweisung übereinstimmt. Jede Regelanweisung gibt je nach Anweisungstyp an, wonach und wie gesucht werden soll.

Jede Regel AWS WAF hat eine einzige Regelanweisung auf oberster Ebene, die weitere Anweisungen enthalten kann. Regelanweisungen können sehr einfach sein. Sie könnten beispielsweise eine Anweisung haben, die eine Reihe von Ursprungsländern angibt, für die Sie Ihre Webanfragen überprüfen können, oder Sie könnten eine Regelanweisung in einer Web-ACL haben, die nur auf eine Regelgruppe verweist. Regelanweisungen können sehr komplex sein. Beispielsweise könnten Sie eine Anweisung haben, die viele andere Anweisungen mit logischen AND-, OR- und NOT-Anweisungen kombiniert.

Verschachteln von Regelanweisungen

AWS WAF unterstützt die Verschachtelung für viele Regelanweisungen, aber nicht für alle. Beispielsweise können Sie eine Regelgruppenanweisung nicht in einer anderen Anweisung verschachteln. Für einige Szenarien müssen Sie Verschachtelung verwenden, z. B. Eingrenzungsanweisungen und logische Anweisungen. Die folgenden Regelanweisungslisten und Regeldetails beschreiben die Verschachtelungsfunktionen und Anforderungen für jede Kategorie und Regel.

Der visuelle Editor für Regeln in der Konsole unterstützt nur eine Verschachtelungsebene für Regelanweisungen. Sie können beispielsweise viele Arten von Anweisungen innerhalb einer logischen AND oder einer OR Regel verschachteln, aber Sie können keine andere AND OR OR-Regel verschachteln, weil dafür eine zweite Verschachtelungsebene erforderlich ist. Um mehrere Verschachtelungsebenen zu implementieren, stellen Sie die Regeldefinition in JSON bereit, entweder über den JSON-Regeleditor in der Konsole oder über die APIs.

Themen

- [Webanforderungskomponenten](#)
- [Eingrenzungsanweisungen](#)
- [Anweisungen, die sich auf ein Set oder eine Regelgruppe beziehen](#)

Webanforderungskomponenten

In diesem Abschnitt werden die Einstellungen beschrieben, die Sie für Regelanweisungen angeben können, die eine Komponente der Webanforderung prüfen. Informationen zur Verwendung finden Sie in den einzelnen Regelanweisungen unter [Statements der Match-Regel](#).

Eine Teilmenge dieser Komponenten kann auch in ratenbasierten Regeln als benutzerdefinierte Aggregationsschlüssel für Anfragen verwendet werden. Weitere Informationen finden Sie unter [Aggregationsoptionen und Schlüssel](#).

Für die Einstellungen der Anforderungskomponente geben Sie den Komponententyp selbst und alle zusätzlichen Optionen an, die Sie je nach Komponententyp auswählen. Wenn Sie beispielsweise einen Komponententyp wählen, der zu prüfenden Text enthält, können Sie Texttransformationen angeben, die Sie anwenden AWS WAF möchten, bevor Sie Ihre Prüfkriterien auswerten.

Note

Sofern nicht anders angegeben, wird eine Webanforderung, die nicht über die in der Regelanweisung angegebene Anforderungskomponente verfügt, so AWS WAF bewertet, dass sie den Regelkriterien nicht entspricht.

Inhalt

- [Anforderungskomponentenoptionen](#)
 - [HTTP-Methode](#)
 - [Einzelner Header](#)
 - [Alle Header](#)
 - [Reihenfolge der Kopfzeilen](#)
 - [Cookies](#)
 - [URI-Pfad](#)
 - [JA3-Fingerabdruck](#)

- [Abfragezeichenfolge](#)
- [Einzelabfrageparameter](#)
- [Alle Abfrageparameter](#)
- [Fließtext](#)
- [JSON-Text](#)
- [Weitergeleitete IP-Adresse](#)
- [Wie man HTTP/2-Pseudo-Header untersucht](#)
- [Texttransformationen](#)

Anforderungskomponentenoptionen

In diesem Abschnitt werden die Komponenten der Webanforderung beschrieben, die Sie prüfen lassen können. Sie legen die Anforderungskomponente für Übereinstimmungsregeln fest, die nach Mustern innerhalb der Webanforderung suchen. Zu diesen Anweisungstypen gehören String-Match-, Regex-Match-, Größenbeschränkungs- und SQL-Injection-Angriffsanweisungen. Informationen zur Verwendung dieser Einstellungen für Anforderungskomponenten finden Sie in den einzelnen Regeln unter [Statements der Match-Regel](#)

Sofern nicht anders angegeben, wird eine Webanforderung, die nicht über die in der Regelanweisung angegebene Anforderungskomponente verfügt, AWS WAF dahingehend bewertet, dass sie den Regelkriterien nicht entspricht.

Note

Sie geben für jede Regelanweisung, die eine solche erfordert, eine einzige Anforderungskomponente an. Um mehr als eine Komponente einer Anforderung zu prüfen, erstellen Sie für jede Komponente eine Regelanweisung.

Die AWS WAF Konsole und die API-Dokumentation enthalten Anleitungen zu den Einstellungen der Anforderungskomponente an den folgenden Stellen:

- Rule Builder in der Konsole – Wählen Sie in den Einstellungen für einen regulären Regeltyp unter Statement (Anweisung) die zu prüfende Komponente unter Request components (Anforderungskomponenten) im Dialog Inspect (Untersuchen) aus.
- API-Anweisungsinhalt – FieldToMatch

Der Rest dieses Abschnitts beschreibt die Optionen für den Teil der Webanforderung, der überprüft werden soll.

Themen

- [HTTP-Methode](#)
- [Einzelner Header](#)
- [Alle Header](#)
- [Reihenfolge der Kopfzeilen](#)
- [Cookies](#)
- [URI-Pfad](#)
- [JA3-Fingerabdruck](#)
- [Abfragezeichenfolge](#)
- [Einzelabfrageparameter](#)
- [Alle Abfrageparameter](#)
- [Fließtext](#)
- [JSON-Text](#)

HTTP-Methode

Prüft die HTTP-Methode der Anforderung. Die HTTP-Methode gibt die Art des Vorgangs an, zu dessen Ausführung die Webanforderung Ihre geschützte Ressource auffordert, z. B. POST oder GET.

Einzelner Header

Prüft einen einzelnen benannten Header in der Anforderung. Für diese Option geben Sie den Header-Namen an, zum Beispiel `User-Agent` oder `Referer`. Bei der Übereinstimmung mit der Zeichenfolge für den Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden.

Alle Header

Prüft alle Anforderungsheader, einschließlich Cookies. Sie können einen Filter anwenden, um eine Teilmenge aller Header zu überprüfen. Für diese Option geben Sie die folgenden Spezifikationen an:

- **Muster zuordnen** — Der Filter, der verwendet werden soll, um eine Teilmenge von Headern zur Überprüfung abzurufen. AWS WAF sucht in den Header-Tasten nach diesen Mustern.

Die Einstellung für Übereinstimmungsmuster kann eine der folgenden sein:

- **All (Alle)** – Übereinstimmung mit allen Schlüsseln. Bewerten Sie die Regelprüfungskriterien für alle Header.
- **Excluded headers (Ausgeschlossene Header)** – Untersuchen Sie nur die Header, deren Schlüssel mit keiner der hier angegebenen Zeichenfolgen übereinstimmen. Bei der Zeichenfolgenübereinstimmung für einen Schlüssel wird nicht zwischen Groß- und Kleinschreibung unterschieden.
- **Included headers (Enthaltene Header)** – Untersuchen Sie nur die Header, deren Schlüssel mit einer der hier angegebenen Zeichenfolgen übereinstimmt. Bei der Zeichenfolgenübereinstimmung für einen Schlüssel wird nicht zwischen Groß- und Kleinschreibung unterschieden.
- **Gültigkeitsbereich** — Die Teile der Header, die anhand der Regelprüfungskriterien geprüft werden AWS WAF sollen. Sie können Schlüssel, Werte oder Alle angeben, um sowohl Schlüssel als auch Werte auf eine Übereinstimmung zu überprüfen.

All erfordert nicht, dass eine Übereinstimmung in den Schlüsseln und eine Übereinstimmung in den Werten gefunden wird. Es erfordert, dass eine Übereinstimmung in den Schlüsseln oder den Werten oder in beiden gefunden wird. Um eine Übereinstimmung in den Schlüsseln und in den Werten zu verlangen, verwenden Sie eine logische AND Anweisung, um zwei Vergleichsregeln zu kombinieren: eine, die die Schlüssel überprüft, und eine andere, die die Werte überprüft.

- **Behandlung zu großer Datenmengen** — Wie AWS WAF soll mit Anfragen umgegangen werden, deren Header-Daten so groß sind, dass sie nicht untersucht werden können? AWS WAF AWS WAF kann höchstens die ersten 8 KB (8.192 Byte) der Anforderungsheader und höchstens die ersten 200 Header untersuchen. Der Inhalt kann AWS WAF bis zum ersten erreichten Limit überprüft werden. Sie können die Untersuchung fortsetzen oder überspringen und die Anforderung als mit der Regel übereinstimmend oder nicht mit der Regel übereinstimmend markieren. Weitere Informationen zur Handhabung zu großen Inhalten finden Sie unter [Umgang mit übergroßen Webanforderungskomponenten in AWS WAF](#).

Reihenfolge der Kopfzeilen

Untersuchen Sie eine Zeichenfolge, die die Liste der Header-Namen der Anfrage enthält, und zwar in der Reihenfolge, in der sie in der Webanforderung erscheinen, die zur AWS WAF Überprüfung geht. AWS WAF generiert die Zeichenfolge und verwendet sie dann als Feld, das der Komponente bei der Prüfung entspricht. AWS WAF trennt die Header-Namen in der Zeichenfolge beispielsweise `host:user-agent:accept:authorization:referer` durch Doppelpunkte und ohne zusätzliche Leerzeichen.

Für diese Option geben Sie die folgenden Spezifikationen an:

- **Behandlung von Übergrößen** — Wie AWS WAF soll mit Anfragen umgegangen werden, deren Header-Daten zahlreicher oder umfangreicher sind, als untersucht AWS WAF werden können? AWS WAF kann höchstens die ersten 8 KB (8.192 Byte) der Anforderungsheader und höchstens die ersten 200 Header untersuchen. Der Inhalt kann AWS WAF bis zum ersten erreichten Limit überprüft werden. Sie können wählen, ob Sie die Überprüfung der verfügbaren Header fortsetzen oder die Überprüfung überspringen und die Anfrage als mit der Regel übereinstimmend oder nicht übereinstimmend markieren möchten. Weitere Informationen zur Handhabung zu großen Inhalten finden Sie unter [Umgang mit übergroßen Webanforderungskomponenten in AWS WAF](#).

Cookies

Prüft alle Anforderungs-Cookies. Sie können einen Filter anwenden, um eine Teilmenge aller Cookies zu überprüfen. Für diese Option geben Sie die folgenden Spezifikationen an:

- **Match patterns (Übereinstimmungsmuster)** – Der Filter, der verwendet werden soll, um eine Teilmenge von Cookies für die Prüfung zu erhalten. AWS WAF sucht nach diesen Mustern in den Header-Cookies.

Die Einstellung für Übereinstimmungsmuster kann eine der folgenden sein:

- **All (Alle)** – Übereinstimmung mit allen Schlüsseln. Bewerten Sie die Regelprüfungskriterien für alle Cookies.
- **Excluded cookies (Ausgeschlossene Cookies)** – Untersuchen Sie nur die Cookies, deren Schlüssel mit keiner der hier angegebenen Zeichenfolgen übereinstimmen. Beim Zeichenfolgenabgleich für einen Schlüssel wird zwischen Groß- und Kleinschreibung unterschieden. Die Übereinstimmung muss exakt sein.
- **Included cookies (Enthaltene Cookies)** – Untersuchen Sie nur die Cookies, deren Schlüssel mit einer der hier angegebenen Zeichenfolgen übereinstimmt. Beim Zeichenfolgenabgleich für einen Schlüssel wird zwischen Groß- und Kleinschreibung unterschieden. Die Übereinstimmung muss exakt sein.
- **Geltungsbereich zuordnen** — Die Teile der Cookies, die anhand der Regelprüfungskriterien überprüft werden AWS WAF sollen. Sie können Keys (Schlüssel), Values (Werte), oder All (Alle) für sowohl Schlüssel als auch Werte angeben.

All erfordert nicht, dass eine Übereinstimmung in den Schlüsseln und eine Übereinstimmung in den Werten gefunden wird. Es erfordert, dass eine Übereinstimmung in den Schlüsseln oder den

Werten oder in beiden gefunden wird. Um eine Übereinstimmung in den Schlüsseln und in den Werten zu verlangen, verwenden Sie eine logische AND Anweisung, um zwei Vergleichsregeln zu kombinieren: eine, die die Schlüssel überprüft, und eine andere, die die Werte überprüft.

- Umgang mit überdimensionalen Daten — Wie AWS WAF soll mit Anfragen umgegangen werden, deren Cookie-Daten größer sind als AWS WAF das, was untersucht werden kann? AWS WAF kann höchstens die ersten 8 KB (8.192 Byte) der Anforderungs-Cookies und höchstens die ersten 200 Cookies untersuchen. Der Inhalt kann AWS WAF bis zur ersten erreichten Grenze eingesehen werden. Sie können die Untersuchung fortsetzen oder überspringen und die Anforderung als mit der Regel übereinstimmend oder nicht mit der Regel übereinstimmend markieren. Weitere Informationen zur Handhabung zu großen Inhalten finden Sie unter [Umgang mit übergroßen Webanforderungskomponenten in AWS WAF](#).

URI-Pfad

Prüft den Teil einer URL, der eine Ressource angibt, z. B. `/images/daily-ad.jpg`. Informationen dazu finden Sie unter [Uniform Resource Identifier \(URI\): Generic Syntax](#).

Wenn Sie mit dieser Option keine Texttransformation verwenden, wird der URI AWS WAF nicht normalisiert und er wird genau so geprüft, wie er ihn vom Client in der Anfrage erhält. Informationen zu Texttransformationen finden Sie unter [Texttransformationen](#).

JA3-Fingerabdruck

Prüft den JA3-Fingerabdruck der Anfrage. Der JA3-Fingerabdruck ist ein 32-stelliger Hash, der vom TLS-Client-Hello einer eingehenden Anfrage abgeleitet wird. Dieser Fingerabdruck dient als eindeutige Kennung für die TLS-Konfiguration des Clients. AWS WAF berechnet und protokolliert diesen Fingerabdruck für jede Anfrage, die genügend TLS-Client-Hello-Informationen für die Berechnung enthält. Fast alle Webanfragen enthalten diese Informationen.

Wie erhalte ich den JA3-Fingerabdruck für einen Kunden

Sie können den JA3-Fingerabdruck für die Anfragen eines Kunden aus den Web-ACL-Protokollen abrufen. Wenn AWS WAF es in der Lage ist, den Fingerabdruck zu berechnen, nimmt es ihn in die Protokolle auf. Hinweise zu den Protokollierungsfeldern finden Sie unter [Protokollfelder](#).

Anforderungen an die Regelerklärung

Sie können den JA3-Fingerabdruck nur in einer Anweisung zur Übereinstimmung mit einer Zeichenfolge überprüfen, die so eingestellt ist, dass sie genau mit der von Ihnen angegebenen Zeichenfolge übereinstimmt. Geben Sie die JA3-Fingerabdruckzeichenfolge aus den Protokollen in

Ihrer String-Match-Anweisungsspezifikation an, um sie mit future Anfragen abzugleichen, die dieselbe TLS-Konfiguration haben. Hinweise zur Anweisung zum Abgleichen von Zeichenketten finden Sie unter [Zeichenfolgen-Übereinstimmungsanweisung](#).

Sie müssen ein Ausweichverhalten für diese Regelanweisung angeben. Das Fallback-Verhalten ist der Übereinstimmungsstatus, den Sie der Webanforderung zuweisen AWS WAF möchten, wenn der AWS WAF JA3-Fingerabdruck nicht berechnet werden kann. Wenn Sie sich für einen Abgleich entscheiden, AWS WAF behandelt die Anfrage so, als ob sie der Regelanweisung entspricht, und wendet die Regelaktion auf die Anfrage an. Wenn Sie keine Übereinstimmung wählen, wird die Anfrage so AWS WAF behandelt, als ob sie nicht mit der Regelanweisung übereinstimmt.

Um diese Match-Option verwenden zu können, müssen Sie Ihren Web-ACL-Verkehr protokollieren. Weitere Informationen finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).

Abfragezeichenfolge

Prüft den Teil der URL nach einem „?“ , sofern vorhanden.

Note

Für standortübergreifende Scripting-Abgleichsanweisungen empfehlen wir, dass Sie Alle Abfrageparameter anstelle von Abfragezeichenfolge wählen. Die Auswahl von All query parameters (Alle Abfrageparameter) fügt den Basiskosten 10 WCUs hinzu.

Einzelabfrageparameter

Prüft einen einzelnen Abfrageparameter, den Sie als Teil der Abfragezeichenfolge definiert haben. AWS WAF überprüft den Wert des von Ihnen angegebenen Parameters.

Für diese Option geben Sie auch ein Query argument (Abfrageargument) an. Wenn die z. B. URL `www.xyz.com?UserName=abc&SalesRegion=seattle` lautet, können Sie für das Abfrageargument `UserName` oder `SalesRegion` angeben. Die maximale Länge des Argumentnamens beträgt 30 Zeichen. Der Name unterscheidet nicht zwischen Groß- und Kleinschreibung. Wenn Sie `UserName` angeben, stimmt AWS WAF also mit allen Varianten von `UserName` überein (einschließlich `username` und `UsERName`).

Wenn die Abfragezeichenfolge mehr als eine Instanz des von Ihnen angegebenen Abfragearguments enthält, werden AWS WAF alle Werte mithilfe OR von Logik auf eine Übereinstimmung überprüft. In der URL `www.xyz.com?SalesRegion=boston&SalesRegion=seattle` bewertet AWS WAF

beispielsweise den Namen, den Sie für `boston` und `seattle` angegeben haben. Wenn eine der beiden Varianten übereinstimmt, ist die Überprüfung eine Übereinstimmung.

Alle Abfrageparameter

Prüft alle Abfrageparameter in der Anforderung. Dies ähnelt der Komponentenauswahl für einen einzelnen Abfrageparameter, AWS WAF überprüft jedoch die Werte aller Argumente innerhalb der Abfragezeichenfolge. Wenn die URL beispielsweise `www.xyz.com?UserName=abc&SalesRegion=seattle` ist, löst AWS WAF eine Übereinstimmung aus, wenn entweder der Wert von `UserName` oder `SalesRegion` den Prüfkriterien entspricht.

Wenn Sie diese Option wählen, werden den Basiskosten 10 WCUs hinzugefügt.

Fließtext

Prüft den Anforderungstext, der als Klartext ausgewertet wird. Sie können den Text auch als JSON-Code auswerten, indem Sie den Inhaltstyp JSON verwenden.

Der Anforderungstext ist der Teil, der unmittelbar auf die Header der Anforderung folgt. Er enthält alle zusätzlichen Daten, die für die Webanforderung benötigt werden, z. B. Daten aus einem Formular.

- In der Konsole wählen Sie dies unter der Request option (Anforderungsoption) Body (Text) aus, indem Sie den Content type (Inhaltstyp) Plain text (Klartext) auswählen.
- In der API geben Sie in der FieldToMatch-Spezifikation der Regel Body an, um den Anforderungstext als Klartext zu untersuchen.

Für Application Load Balancer und AWS AppSync AWS WAF können die ersten 8 KB des Hauptteils einer Anfrage untersuchen. Denn CloudFront API Gateway, Amazon Cognito, App Runner und Verified Access AWS WAF können standardmäßig die ersten 16 KB überprüfen, und Sie können das Limit in Ihrer Web-ACL-Konfiguration auf bis zu 64 KB erhöhen. Weitere Informationen finden Sie unter [Verwaltung der Größenbeschränkungen bei Körperinspektionen](#).

Sie müssen für diesen Komponententyp die Handhabung zu großer Inhalte angeben. Die Verarbeitung von Übergrößen definiert, wie Anfragen AWS WAF behandelt werden, deren Hauptdaten größer sind als das, was untersucht AWS WAF werden kann. Sie können die Untersuchung fortsetzen oder überspringen und die Anforderung als mit der Regel übereinstimmend oder nicht mit der Regel übereinstimmend markieren. Weitere Informationen zur Handhabung zu großen Inhalten finden Sie unter [Umgang mit übergroßen Webanforderungskomponenten in AWS WAF](#).

Sie können den Text auch als analysierten JSON-Code bewerten. Informationen zu diesem Konto finden Sie im folgenden Abschnitt.

JSON-Text

Prüft den Anforderungstext, der als JSON-Code ausgewertet wird. Sie können den Text auch als Klartext auswerten.

Der Anforderungstext ist der Teil, der unmittelbar auf die Header der Anforderung folgt. Er enthält alle zusätzlichen Daten, die für die Webanforderung benötigt werden, z. B. Daten aus einem Formular.

- In der Konsole wählen Sie dies unter der Request option (Anforderungsoption) Body (Text) aus, indem Sie den Content type (Inhaltstyp) JSON auswählen.
- In der API geben Sie in der FieldToMatch-Spezifikation der Regel JsonBody an.

Für Application Load Balancer und AWS AppSync AWS WAF können die ersten 8 KB des Hauptteils einer Anfrage untersuchen. Denn CloudFront API Gateway, Amazon Cognito, App Runner und Verified Access AWS WAF können standardmäßig die ersten 16 KB überprüfen, und Sie können das Limit in Ihrer Web-ACL-Konfiguration auf bis zu 64 KB erhöhen. Weitere Informationen finden Sie unter [Verwaltung der Größenbeschränkungen bei Körperinspektionen](#).

Sie müssen für diesen Komponententyp die Handhabung zu großer Inhalte angeben. Die Verarbeitung von Übergrößen definiert, wie Anfragen AWS WAF behandelt werden, deren Hauptdaten größer sind als das, was untersucht AWS WAF werden kann. Sie können die Untersuchung fortsetzen oder überspringen und die Anforderung als mit der Regel übereinstimmend oder nicht mit der Regel übereinstimmend markieren. Weitere Informationen zur Handhabung zu großen Inhalten finden Sie unter [Umgang mit übergroßen Webanforderungskomponenten in AWS WAF](#).

Wenn der AWS WAF Hauptteil der Webanfrage als geparstes JSON geprüft wird, analysiert und extrahiert es die Elemente aus dem JSON und überprüft die Teile, die Sie anhand der Match-Statement-Kriterien der Regel angeben.

Wenn Sie diese Option wählen, verdoppeln sich die Basiskosten-WCUs der Übereinstimmungsanweisung. Wenn beispielsweise die Basiskosten der Übereinstimmungsanweisung ohne JSON-Analyse 5 WCUs betragen, verdoppeln sich die Kosten mit JSON-Analyse auf 10 WCUs.

Bei dieser Option werden zwei Vergleichsmuster für den Hauptteil der Webanfrage AWS WAF ausgeführt. Die Ausgabe des ersten Übereinstimmungsmusters wird als Eingabe für das zweite Übereinstimmungsmuster verwendet:

1. AWS WAF analysiert und extrahiert den JSON-Inhalt und identifiziert die zu untersuchenden Elemente. AWS WAF verwendet dazu die Kriterien, die Sie in der JSON-Textspezifikation der Regel angeben.
2. AWS WAF wendet alle Texttransformationen auf die extrahierten Elemente an und gleicht dann den resultierenden JSON-Elementsatz mit den Übereinstimmungskriterien der Regelanweisung ab. Falls eines der Elemente übereinstimmt, ist die Webanforderung eine Übereinstimmung mit der Regel.

Sie geben die folgenden Kriterien an AWS WAF, die für den ersten Schritt des Mustervergleichs verwendet werden sollen, um die zu untersuchenden JSON-Elemente zu identifizieren:

- Body parsing fallback behavior (Fallback-Verhalten beim Analysieren des Texts) – Was AWS WAF tun soll, wenn es den JSON-Text nicht vollständig analysieren kann. Es gibt die folgenden Optionen:
 - Keine (Standardverhalten) — AWS WAF wertet den Inhalt nur bis zu dem Punkt aus, an dem ein Analysefehler aufgetreten ist.
 - Als Zeichenfolge auswerten — Untersuchen Sie den Textkörper als reinen Text. AWS WAF wendet die Texttransformationen und Prüfkriterien, die Sie für die JSON-Prüfung definiert haben, auf die Texttextzeichenfolge an.
 - Abgleichen — Behandelt die Webanforderung so, als ob sie der Regelanweisung entspricht. AWS WAF wendet die Regelaktion auf die Anfrage an.
 - No Match (Keine Übereinstimmung) – Behandelt die Webanforderung als nicht mit der Regelanweisung übereinstimmend.

AWS WAF versucht nach besten Kräften, den gesamten JSON-Hauptteil zu analysieren, kann aber aus Gründen wie ungültigen Zeichen, doppelten Schlüsseln, Kürzungen und Inhalten, deren Stammknoten kein Objekt oder Array ist, zum Abbruch gezwungen werden.

AWS WAF analysiert den JSON-Code in den folgenden Beispielen als zwei gültige Schlüssel:Wert-Paare:

- Fehlendes Komma: {"key1":"value1""key2":"value2"}
- Fehlender Doppelpunkt: {"key1":"value1", "key2""value2"}

- Zusätzliche Doppelpunkte: {"key1": "value1", "key2": "value2"}
- JSON-Match-Bereich — Die Typen von Elementen im JSON, AWS WAF die überprüft werden sollen. Sie können Keys (Schlüssel), Values (Werte), oder All (Alle) für sowohl Schlüssel als auch Werte angeben.

All erfordert nicht, dass eine Übereinstimmung in den Schlüsseln und eine Übereinstimmung in den Werten gefunden wird. Es erfordert, dass eine Übereinstimmung in den Schlüsseln oder den Werten oder in beiden gefunden wird. Um eine Übereinstimmung in den Schlüsseln und in den Werten zu verlangen, verwenden Sie eine logische AND Anweisung, um zwei Vergleichsregeln zu kombinieren: eine, die die Schlüssel überprüft, und eine andere, die die Werte überprüft.

- Zu untersuchender Inhalt — Die Elemente in der analysierten und extrahierten JSON-Datei, die Sie untersuchen möchten AWS WAF .

Sie müssen eine der folgenden Eigenschaften angeben:

- Full JSON content (Vollständiger JSON-Inhalt) – Alle Elemente im analysierten JSON-Code auswerten.
- Only included elements (Nur enthaltene Elemente) – Nur Elemente im JSON-Code auswerten, die den von Ihnen angegebenen JSON-Pointer-Kriterien entsprechen. Informationen zur JSON-Pointer-Syntax finden Sie in der Dokumentation [JavaScript Object Notation \(JSON\) Pointer \(JSON\) der Internet Engineering Task Force \(IETF\)](#).

Verwenden Sie diese Option nicht, um alle Pfade im JSON-Code einzubeziehen. Verwenden Sie stattdessen Full JSON content (Vollständiger JSON-Inhalt).

Sie können beispielsweise in der Konsole Folgendes eingeben:

```
/dogs/0/name  
/dogs/1/name
```

In der API oder CLI können Sie Folgendes angeben:

```
"IncludedPaths": ["/dogs/0/name", "/dogs/1/name"]
```

Beispielszenario für die Überprüfung des JSON-Texts

Wenn die Einstellung für eingeschlossene Elemente /a/b lautet, dann für den folgenden JSON-Text:

```
{
  "a": {
    "c": "d",
    "b": {
      "e": {
        "f": "g"
      }
    }
  }
}
```

In der folgenden Liste wird beschrieben, was für jede Einstellung des Übereinstimmungsbereichs ausgewertet werden AWS WAF würde. Der Schlüssel b, der Teil des Pfads der eingeschlossenen Elemente ist, wird nicht ausgewertet.

- Übereinstimmungsbereich auf alle gesetzt: e, f, und g.
- Übereinstimmungsbereich auf Schlüssel gesetzt: e und f.
- Übereinstimmungsbereich auf Werte gesetzt: g.

Weitergeleitete IP-Adresse

Dieser Abschnitt gilt für Regelnweisungen, die die IP-Adresse einer Webanforderung verwenden. AWS WAF verwendet standardmäßig die IP-Adresse aus dem Ursprung der Webanfrage. Wenn eine Webanforderung jedoch einen oder mehrere Proxys oder Load Balancer durchläuft, enthält der Ursprung der Webanforderung die Adresse des letzten Proxys und nicht die Ursprungsadresse des Clients. In diesem Fall wird die ursprüngliche Clientadresse normalerweise in einem anderen HTTP-Header weitergeleitet. Dieser Header ist normalerweise X-Forwarded-For (XFF), es kann aber auch ein anderer sein.

Regelanweisungen, die IP-Adressen verwenden

Folgende Regelanweisungen verwenden IP-Adressen:

- [IP-Set-Übereinstimmung](#) – Prüft die IP-Adresse auf eine Übereinstimmung mit den Adressen, die in einem IP-Set definiert sind.
- [Geographische Übereinstimmung](#)- Verwendet die IP-Adresse, um das Herkunftsland und die Herkunftsregion zu bestimmen, und vergleicht das Herkunftsland mit einer Liste von Ländern.
- [Ratenbasierte Regelanweisung](#)- Kann Anfragen nach ihren IP-Adressen zusammenfassen, um sicherzustellen, dass keine einzelne IP-Adresse Anfragen mit zu hoher Geschwindigkeit

sendet. Sie können die IP-Adressaggregation allein oder in Kombination mit anderen Aggregationsschlüsseln verwenden.

Sie können anweisen AWS WAF, für jede dieser Regeln eine weitergeleitete IP-Adresse zu verwenden, entweder aus dem `X-Forwarded-For` Header oder aus einem anderen HTTP-Header, anstatt den Ursprung der Webanfrage zu verwenden. Einzelheiten zur Bereitstellung der Spezifikationen finden Sie in den Empfehlungen zu den einzelnen Regelausweisungstypen.

Note

Wenn der von Ihnen angegebene Header in der Anfrage nicht vorhanden ist, wird die Regel überhaupt AWS WAF nicht auf die Webanforderung angewendet.

Fallback-Verhalten

Wenn Sie die weitergeleitete IP-Adresse verwenden, geben Sie den Übereinstimmungsstatus AWS WAF an, der der Webanfrage zugewiesen werden soll, falls die Anfrage an der angegebenen Position keine gültige IP-Adresse hat:

- **MATCH** — Behandelt die Webanforderung so, als ob sie der Regelanweisung entspricht. AWS WAF wendet die Regelaktion auf die Anfrage an.
- **KEINE ÜBEREINSTIMMUNG** — Behandelt die Webanforderung als nicht übereinstimmend mit der Regelanweisung.

In AWS WAF Bot Control verwendete IP-Adressen

Die von Bot Control verwaltete Regelgruppe verifiziert Bots anhand der IP-Adressen von AWS WAF. Wenn Sie Bot Control verwenden und verifizierte Bots haben, die durch einen Proxy oder Load Balancer geleitet werden, müssen Sie sie explizit mit einer benutzerdefinierten Regel zulassen. Sie können beispielsweise eine benutzerdefinierte IP-Set-Abgleichregel konfigurieren, die Ihre verifizierten Bots anhand weitergeleiteter IP-Adressen erkennt und zulässt. Mit der Regel können Sie Ihre Bot-Verwaltung auf verschiedene Arten anpassen. Weitere Informationen und Beispiele finden Sie unter [AWS WAF Bot-Steuerung](#).

Allgemeine Überlegungen zur Verwendung weitergeleiteter IP-Adressen

Bedenken Sie Folgendes, bevor Sie eine weitergeleitete IP-Adresse verwenden:

- Ein Header kann auf dem Weg von Proxys geändert werden, und die Proxys behandeln den Header möglicherweise auf verschiedene Arten.
- Angreifer können den Inhalt des Headers ändern, um AWS WAF -Inspektionen zu umgehen.
- Die IP-Adresse im Header kann fehlerhaft oder ungültig sein.
- Der von Ihnen angegebene Header ist möglicherweise überhaupt nicht in einer Anforderung vorhanden.

Überlegungen zur Verwendung weitergeleiteter IP-Adressen mit AWS WAF

In der folgenden Liste werden die Anforderungen und Vorbehalte für die Verwendung weitergeleiteter IP-Adressen in AWS WAF folgenden Bereichen beschrieben:

- Für jede einzelne Regel können Sie einen Header für die weitergeleitete IP-Adresse angeben. Bei der Header-Spezifikation wird zwischen Groß- und Kleinschreibung unterschieden.
- Bei ratenbasierten Regeln übernehmen verschachtelte Eingrenzungsanweisungen die weitergeleitete IP-Konfiguration nicht. Geben Sie die Konfiguration für jede Anweisung an, die eine weitergeleitete IP-Adresse verwendet.
- AWS WAF verwendet für Geo-Match- und ratenbasierte Regeln die erste Adresse in der Kopfzeile. Wenn eine Kopfzeile beispielsweise Verwendungen enthält `10.1.1.1`, `127.0.0.0`, `10.10.10.10` AWS WAF `10.1.1.1`
- Für einen IP-Set-Abgleich geben Sie an, ob ein Abgleich mit der ersten, letzten oder irgendeiner Adresse im Header durchgeführt werden soll. Wenn Sie eine angeben, werden alle AWS WAF Adressen in der Kopfzeile auf eine Übereinstimmung überprüft, bis zu 10 Adressen. Wenn die Kopfzeile mehr als 10 Adressen enthält, werden die letzten AWS WAF 10 überprüft.
- Bei Headern mit mehreren Adressen müssen die einzelnen Adressen durch Kommata getrennt sein. Wenn eine Anforderung ein anderes Trennzeichen als ein Komma verwendet, betrachtet AWS WAF die IP-Adressen im Header als fehlerhaft.
- Wenn die IP-Adressen im Header fehlerhaft oder ungültig sind, bezeichnet AWS WAF die Webanforderung entsprechend dem Fallback-Verhalten, das Sie in der Konfiguration für weitergeleitete IP-Adressen angeben, als mit der Regel übereinstimmend oder nicht.
- Wenn der von Ihnen angegebene Header in einer Anfrage nicht vorhanden ist, AWS WAF wird die Regel überhaupt nicht auf die Anfrage angewendet. Das AWS WAF bedeutet, dass die Regelaktion nicht angewendet wird und das Fallback-Verhalten nicht angewendet wird.
- Eine Regelnweisung, die einen weitergeleiteten IP-Header für die IP-Adresse verwendet, verwendet nicht die IP-Adresse, die vom Ursprung der Webanforderung gemeldet wird.

Bewährte Methoden für die Verwendung weitergeleiteter IP-Adressen mit AWS WAF

Halten Sie sich an die folgenden bewährten Methoden, wenn Sie weitergeleitete IP-Adressen verwenden:

- Berücksichtigen Sie sorgfältig alle möglichen Status Ihrer Anforderungsheader, bevor Sie die Konfiguration für weitergeleitete IP-Adressen aktivieren. Möglicherweise müssen Sie mehr als eine Regel verwenden, um das gewünschte Verhalten zu erhalten.
- Verwenden Sie für jede IP-Adressquelle eine Regel, um mehrere weitergeleitete IP-Header zu überprüfen oder den Ursprung der Webanforderung und einen weitergeleiteten IP-Header zu überprüfen.
- Zum Blockieren der Webanforderungen mit ungültigen Headern stellen Sie die Regelaktion auf Blockieren und das Fallback-Verhalten für die Konfiguration für weitergeleitete IP-Adressen entsprechend ein.

Beispiel-JSON-Code für weitergeleitete IP-Adressen

Die folgende Geo-Übereinstimmungsanweisung stimmt nur überein, falls der X-Forwarded-For-Header eine IP enthält, deren Herkunftsland die US sind:

```
{
  "Name": "XFFTestGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestGeo"
  },
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ],
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

```
}  
}
```

Die folgende ratenbasierte Regel aggregiert Anforderungen basierend auf der ersten IP im X-Forwarded-For-Header. Die Regel zählt nur Anfragen, die mit der verschachtelten Geo-Match-Anweisung übereinstimmen, und blockiert nur Anfragen, die der Geo-Match-Anweisung entsprechen. Die verschachtelte Geo-Übereinstimmungsanweisung stellt außerdem anhand des X-Forwarded-For-Headers fest, ob die IP-Adresse aus den US stammt. Falls dies der Fall ist oder der Header vorhanden, aber fehlerhaft ist, gibt die Geo-Übereinstimmungsanweisung eine Übereinstimmung zurück.

```
{  
  "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"  
      }  
    }  
  }  
}
```

```
}
}
```

Wie man HTTP/2-Pseudo-Header untersucht

Geschützte AWS Ressourcen, die HTTP/2-Verkehr unterstützen, leiten HTTP/2-Pseudo-Header nicht AWS WAF zur Überprüfung weiter, sondern stellen den Inhalt von Pseudo-Headern in Webanforderungskomponenten bereit, die Inspektionen durchführen. AWS WAF Sie können diese Option verwenden AWS WAF , um nur die Pseudo-Header zu untersuchen, die in der folgenden Tabelle aufgeführt sind.

HTTP/2-Pseudo-Header-Inhalte, die Webanforderungskomponenten zugeordnet sind

HTTP/2-Pseudo-Header	Zu inspizierende Webanforderungskomponente	Dokumentation
:method	HTTP-Methode	HTTP-Methode
:authority	Host-Header	Einzelner Header Alle Header
:path	URI-Pfad	URI-Pfad
:path query	Abfragezeichenfolge	Abfragezeichenfolge Einzelabfrageparameter Alle Abfrageparameter

Texttransformationen

In Anweisungen, die nach Mustern suchen oder Einschränkungen festlegen, können Sie Transformationen angeben, die angewendet werden sollen, bevor AWS WAF die Anfrage geprüft wird. Eine Transformation formatiert eine Webanforderung neu, um einige der unüblichen Formatierungen zu beseitigen, die Angreifer verwenden, um AWS WAF zu umgehen.

Wenn Sie dies mit der Auswahl der JSON-Text-Anforderungskomponente verwenden, wendet AWS WAF Ihre Transformationen nach dem Analysieren und Extrahieren der zu prüfenden Elemente aus dem JSON-Code an. Weitere Informationen finden Sie unter [JSON-Text](#).

Wenn Sie mehr als eine Transformation bereitstellen, legen Sie auch die Reihenfolge fest, in der AWS WAF sie anwenden soll.

WCUs – Jede Texttransformation besteht aus 10 WCUs.

Die AWS WAF Konsole und die API-Dokumentation enthalten außerdem Anleitungen zu diesen Einstellungen an den folgenden Stellen:

- Rule Builder in der Konsole – Text transformation (Texttransformation). Diese Option ist verfügbar, wenn Sie Anforderungskomponenten verwenden.
- API-Anweisungsinhalt – `TextTransformations`

Optionen für Texttransformationen

Jede Transformationsliste enthält die Konsolen- und API-Spezifikationen, gefolgt von der Beschreibung.

Base64 decode – `BASE64_DECODE`

AWS WAF dekodiert eine Base64-kodierte Zeichenfolge.

Base64 decode extension – `BASE64_DECODE_EXT`

AWS WAF dekodiert eine Base64-kodierte Zeichenfolge, verwendet jedoch eine fehlerverzeihende Implementierung, die ungültige Zeichen ignoriert.

Command line – `CMD_LINE`

Diese Option entschärft Situationen, in denen Angreifer möglicherweise einen Befehlszeilenbefehl des Betriebssystems eingeben und ungewöhnliche Formatierungen verwenden, um den Befehl ganz oder teilweise zu verschleiern.

Verwenden Sie diese Option, um die folgenden Transformationen durchzuführen:

- Löschen der folgenden Zeichen: \ " ' ^
- Löschen von Leerzeichen vor den folgenden Zeichen: / (
- Ersetzen der folgenden Zeichen durch ein Leerzeichen: , ;

- Ersetzen mehrerer Leerzeichen durch ein Leerzeichen
- Großbuchstaben (A-Z) in Kleinbuchstaben (a-z) umwandeln

Compress whitespace – COMPRESS_WHITE_SPACE

AWS WAF komprimiert Leerzeichen, indem mehrere Leerzeichen durch ein Leerzeichen und die folgenden Zeichen durch ein Leerzeichen (ASCII 32) ersetzt werden:

- Formfeed (ASCII 12)
- Registerkarte (ASCII 9)
- Neue Zeile (ASCII 10)
- Wagenrückfahrt (ASCII 13)
- Vertikaler Tabulator (ASCII 11)
- Sicheres Leerzeichen (ASCII 160)

CSS decode – CSS_DECODE

AWS WAF dekodiert Zeichen, die mit CSS 2.x-Escape-Regeln codiert wurden.

`syndata.html#characters` Diese Funktion verwendet bei der DeCodierung bis zu zwei Bytes, sodass ASCII-Zeichen aufgedeckt werden können, die mit CSS-Codierung codiert wurden und normalerweise nicht codiert werden würden. Sie ist auch nützlich, um eine Umgehung zu verhindern, also eine Kombination aus einem Rückwärtsschrägstrich und nicht-hexadezimalen Zeichen. Beispielsweise `ja\vascript` für `javascript`.

Escape sequences decode – ESCAPE_SEQ_DECODE

AWS WAF dekodiert die folgenden ANSI C-Escape-Sequenzen: `\a,,\b,\f,,\n,\r,, \t \v\\`, `\xHH` (hexadezimal) `\? \'\"`, (oktal). `\0000` Ungültige Codierungen verbleiben in der Ausgabe.

Hex decode – HEX_DECODE

AWS WAF dekodiert eine Folge von Hexadezimalzeichen in eine Binärdatei.

HTML entity decode – HTML_ENTITY_DECODE

AWS WAF ersetzt Zeichen, die im Hexadezimalformat `&#xhhhh;` oder Dezimalformat dargestellt werden, durch die entsprechenden Zeichen. `&#nnnn;`

AWS WAF ersetzt die folgenden HTML-codierten Zeichen durch unkodierte Zeichen. In dieser Liste wird HTML-Kodierung in Kleinbuchstaben verwendet, bei der Behandlung wird jedoch beispielsweise nicht zwischen Groß- und Kleinschreibung unterschieden und sie werden genauso behandelt. `&QuOt;` `"`

HTML-codiertes Zeichen	ersetzt durch...
"	"
&	&
<	<
>	>
 oder 	geschütztes Leerzeichen, Dezimalzahl 160

	\n, Dezimalzahl 10
		\t, Dezimalzahl 9
&lcurly; oder {	{
|, | oder &Vertical Line;	
} oder }	}
!	!
#	#
$	\$
&percent; oder %	%
'	\
((
))
* oder *	*
+	+

HTML-codiertes Zeichen	ersetzt durch...
<code>&comma;</code>	,
<code>&period;</code>	.
<code>&sol;</code>	/
<code>&colon;</code>	:
<code>&semi;</code>	;
<code>&equals;</code>	=
<code>&quest;</code>	?
<code>&tilde;</code> oder <code>&DiacriticalTilde;</code>	~
<code>&minus;</code>	-
<code>&lsqb;</code> oder <code>&lbrack;</code>	[
<code>&bsol;</code>	\\
<code>&rsqb;</code> oder <code>&rbrack;</code>]
<code>&hat;</code>	^
<code>&lowbar;</code> oder <code>&underbar;</code>	—
<code>&grave;</code> oder <code>&DiacriticalGrave;</code>	`

JS decode – JS_DECODE

AWS WAF dekodiert JavaScript Escape-Sequenzen. Falls sich im ASCII-Codebereich mit voller Zeichenbreite von `\uHHHH` ein `FF01-FF5E`-Code befindet, wird das höhere Byte verwendet, um das untere Byte zu erkennen und anzupassen. Wenn nicht, wird nur das niedrigere Byte verwendet und das höhere Byte wird auf Null gesetzt, was zu einem möglichen Datenverlust führt.

Lowercase – LOWERCASE

AWS WAF wandelt Großbuchstaben (A-Z) in Kleinbuchstaben (a-z) um.

MD5 – MD5

AWS WAF berechnet einen MD5-Hash aus den Daten in der Eingabe. Der berechnete Hash liegt in einer rohen binären Form vor.

None – NONE

AWS WAF überprüft die Webanforderung so, wie sie empfangen wurde, ohne Texttransformationen.

Normalize path – NORMALIZE_PATH

AWS WAF normalisiert die Eingabezeichenfolge, indem mehrere Schrägstriche, Verzeichnis-Selbstverweise und Verzeichnisrückverweise entfernt werden, die nicht am Anfang der Eingabe stehen.

Normalize path Windows – NORMALIZE_PATH_WIN

AWS WAF konvertiert Backslash-Zeichen in Schrägstriche und verarbeitet dann die resultierende Zeichenfolge mithilfe der Transformation. `NORMALIZE_PATH`

Remove nulls – REMOVE_NULLS

AWS WAF entfernt alle NULL Byte aus der Eingabe.

Replace comments – REPLACE_COMMENTS

AWS WAF ersetzt jedes Vorkommen eines Kommentars im C-Stil (`/*... */`) durch ein einzelnes Leerzeichen. Mehrere aufeinanderfolgende Vorkommen werden nicht komprimiert. Nicht beendete Kommentare werden durch ein Leerzeichen (ASCII 0x20) ersetzt. Eigenständige Beendigungen von Kommentaren (`*/`) werden nicht geändert.

Replace nulls – REPLACE_NULLS

AWS WAF ersetzt jedes NULL Byte in der Eingabe durch das Leerzeichen (ASCII 0x20).

SQL hex decode – SQL_HEX_DECODE

AWS WAF dekodiert SQL-Hex-Daten. AWS WAF Dekodiert beispielsweise (`0x414243`) nach (ABC).

URL decode – URL_DECODE

AWS WAF dekodiert einen URL-codierten Wert.

URL decode Unicode – URL_DECODE_UNI

Wie URL_DECODE, aber mit Unterstützung für Microsoft-spezifische %u-Kodierung. Falls sich der Code im ASCII-Codebereich mit voller Zeichenbreite von FF01–FF5E befindet, wird das höhere Byte verwendet, um das untere Byte zu erkennen und anzupassen. Andernfalls wird nur das niedrigere Byte verwendet und das höhere Byte wird auf Null gesetzt.

UTF8 to Unicode – UTF8_TO_UNICODE

AWS WAF konvertiert alle UTF-8-Zeichenfolgen nach Unicode. Dies hilft bei der Normalisierung von Eingaben und minimiert Falsch-Positives und Falsch-Negatives für nicht-englische Sprachen.

Eingrenzungsanweisungen

Eine Scope-Down-Anweisung ist eine verschachtelte Regelanweisung, die Sie in eine verwaltete Regelgruppenanweisung oder eine ratenbasierte Anweisung einfügen, um die Menge der Anfragen einzugrenzen, die die enthaltende Regel auswertet. Die enthaltende Regel wertet nur die Anforderungen aus, die zuerst der Scopedown-Anweisung entsprechen.

- Anweisung für verwaltete Regelgruppen — Wenn Sie einer Anweisung für verwaltete Regelgruppen eine Scope-Down-Anweisung hinzufügen, wird jede Anforderung, die nicht mit der Scope-Down-Anweisung übereinstimmt, als nicht mit der Regelgruppe übereinstimmend AWS WAF bewertet. Nur Anforderungen, die der Eingrenzungsanweisung entsprechen, werden anhand der Regelgruppe ausgewertet. Für verwaltete Regelgruppen mit Preisen, die auf der Anzahl der ausgewerteten Anforderungen basieren, können Eingrenzungsanweisungen dazu beitragen, Kosten einzudämmen.

Weitere Informationen zu verwalteten Regelgruppenanweisungen finden Sie unter [Verwaltete Regelgruppenanweisung](#).

- Ratenbasierte Regelaussage — Eine ratenbasierte Regelanweisung ohne Angabe des Umfangs schränkt alle Anfragen ein, die von der Regel ausgewertet werden. Wenn Sie die Rate nur für eine bestimmte Kategorie von Anfragen kontrollieren möchten, fügen Sie der ratenbasierten Regel eine Angabe zum Umfang hinzu. Wenn Sie beispielsweise nur die Rate von Anfragen aus einem bestimmten geografischen Gebiet verfolgen und kontrollieren möchten, können Sie dieses geografische Gebiet in einer geographischen Zuordnung angeben und es Ihrer ratenbasierten Regel als Scopedown-Aussage hinzufügen.

Weitere Informationen über ratenbasierte Regeln finden Sie unter [Ratenbasierte Regeln](#).

in Eingrenzungsanweisungen können Sie jede verschachtelbare Regel verwenden. Die verfügbaren Kontoauszüge finden Sie unter und. [Statements der Match-Regel](#) [Logische Regelaussagen](#) Die WCUs für eine Scope-Down-Anweisung sind die WCUs, die für die Regelanweisung erforderlich sind, die Sie darin definieren. Für die Verwendung einer Scope-Down-Erklärung fallen keine zusätzlichen Kosten an.

Sie können eine Scope-Down-Anweisung genauso konfigurieren, wie Sie es tun, wenn Sie die Anweisung in einer regulären Regel verwenden. Sie können beispielsweise Texttransformationen auf eine Webanforderungskomponente anwenden, die Sie untersuchen, und Sie können eine weitergeleitete IP-Adresse angeben, die als IP-Adresse verwendet werden soll. Diese Konfigurationen gelten nur für die Scope-Down-Anweisung und werden nicht von der zugehörigen verwalteten Regelgruppe oder der ratenbasierten Regelanweisung übernommen.

Wenn Sie beispielsweise Texttransformationen auf eine Abfragezeichenfolge in Ihrer Scope-Down-Anweisung anwenden, überprüft die Scope-Down-Anweisung die Abfragezeichenfolge nach der Anwendung der Transformationen. Wenn die Anforderung den Kriterien der Scope-Down-Anweisung entspricht, AWS WAF wird die Webanforderung in ihrem ursprünglichen Zustand, ohne die Transformationen der Scope-Down-Anweisung, an die enthaltene Regel übergeben. Die Regel, die die Scope-Down-Anweisung enthält, wendet möglicherweise eigene Texttransformationen an, erbt aber keine von der Scope-Down-Anweisung.

Sie können keine Scope-Down-Anweisung verwenden, um eine Konfiguration zur Anforderungsprüfung für die Anweisung, die die Regel enthält, anzugeben. Sie können eine Scope-Down-Anweisung nicht als Präprozessor für Webanfragen für die enthaltene Regelanweisung verwenden. Die einzige Rolle einer Scope-Down-Anweisung besteht darin, zu bestimmen, welche Anfragen zur Überprüfung an die Anweisung, die die Regel enthält, weitergeleitet werden.

Anweisungen, die sich auf ein Set oder eine Regelgruppe beziehen

Einige Regeln verwenden wiederverwendbare Entitäten, die außerhalb Ihrer Web-ACLs verwaltet werden, entweder von Ihnen oder einem AWS Marketplace Verkäufer. AWS Wenn die wiederverwendbare Entität aktualisiert wird, überträgt AWS WAF die Aktualisierung an Ihre Regel. Wenn Sie beispielsweise eine Regelgruppe mit AWS verwalteten Regeln in einer Web-ACL verwenden, wird bei der AWS Aktualisierung der Regelgruppe die Änderung AWS an Ihre Web-ACL weitergegeben, um deren Verhalten zu aktualisieren. Wenn Sie in einer Regel eine IP-Set-

Anweisung verwenden, wird die Änderung bei der Aktualisierung des Satzes auf alle Regeln AWS WAF übertragen, die darauf verweisen, sodass alle Web-ACLs, die diese Regeln verwenden, up-to-date bei Ihren Änderungen beibehalten werden.

Im Folgenden finden Sie die wiederverwendbaren Entitäten, die Sie in einer Regelanweisung verwenden können.

- IP-Sets – Sie erstellen und verwalten Ihre eigenen IP-Sets. In der Konsole können Sie über den Navigationsbereich darauf zugreifen. Informationen zur Verwaltung von IP-Sets finden Sie unter [IP-Sätze und Regex-Mustersätze in AWS WAF](#).
- Regex-Match-Sets – Sie erstellen und verwalten Ihre eigenen Regex-Match-Sets. In der Konsole können Sie über den Navigationsbereich darauf zugreifen. Informationen zur Verwaltung von Regex-Mustersätzen finden Sie unter [IP-Sätze und Regex-Mustersätze in AWS WAF](#).
- AWS Regelgruppen für verwaltete Regeln — AWS verwaltet diese Regelgruppen. In der Konsole stehen Ihnen diese zur Verfügung, wenn Sie Ihrer Web-ACL eine verwaltete Regelgruppe hinzufügen. Weitere Informationen dazu finden Sie unter [AWS Liste der Regelgruppen für verwaltete Regeln](#).
- AWS Marketplace verwaltete Regelgruppen — AWS Marketplace Verkäufer verwalten diese Regelgruppen und Sie können sie abonnieren, um sie zu verwenden. Um Ihre Abonnements zu verwalten, wählen Sie im Navigationsbereich der Konsole AWS Marketplace. Die AWS Marketplace verwalteten Regelgruppen werden aufgelistet, wenn Sie Ihrer Web-ACL eine verwaltete Regelgruppe hinzufügen. Für Regelgruppen, die Sie noch nicht abonniert haben, finden Sie AWS Marketplace auf dieser Seite auch einen Link. Weitere Informationen zu AWS Marketplace vom Verkäufer verwalteten Regelgruppen finden Sie unter [AWS Marketplace verwaltete Regelgruppen](#).
- Ihre eigenen Regelgruppen – Sie verwalten Ihre eigenen Regelgruppen. Dies geschieht normalerweise, wenn Sie ein Verhalten benötigen, das über die verwalteten Regelgruppen nicht verfügbar ist. In der Konsole können Sie über den Navigationsbereich darauf zugreifen. Weitere Informationen finden Sie unter [Verwaltung Ihrer eigenen Regelgruppen](#).

Löschen eines referenzierten Sets oder einer Regelgruppe

Wenn Sie eine Entität löschen, auf die verwiesen wird, wird AWS WAF überprüft, ob sie derzeit in einer Web-ACL verwendet wird. Wenn AWS WAF festgestellt wird, dass sie verwendet wird, werden Sie gewarnt. AWS WAF kann fast immer feststellen, ob eine Web-ACL auf eine Entität verweist. In seltenen Fällen ist dies jedoch nicht möglich. Wenn Sie sicherstellen müssen, dass die zu löschende Entität nicht verwendet wird, überprüfen Sie sie in Ihren Web-ACLs, bevor Sie sie löschen.

Statements der Match-Regel

Match-Anweisungen vergleichen die Webanforderung oder ihren Ursprung mit den von Ihnen angegebenen Kriterien. Bei vielen Anweisungen dieses Typs wird eine bestimmte Komponente der Anfrage nach passenden Inhalten AWS WAF verglichen.

Übereinstimmungsanweisungen sind schachtelbar. Sie können jede dieser Anweisungen in logischen Regelanweisungen verschachteln und sie in Scopedown-Anweisungen verwenden. Hinweise zu logischen Regelanweisungen finden Sie unter [Logische Regelaussagen](#) Informationen zu Eingrenzungsanweisungen finden Sie unter [Eingrenzungsanweisungen](#).

Diese Tabelle beschreibt die regulären Match-Anweisungen, die Sie zu einer Regel hinzufügen können, und enthält einige Richtlinien für die Berechnung der Nutzung von Web ACL Capacity Units (WCU) für jede Regel. Informationen zu den WCUs finden Sie unter [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#).

Übereinstimmungsanweisung	Beschreibung	WCUs
Geographische Übereinstimmung	Überprüft das Ursprungsland der Anfrage und bringt Kennzeichnungen für das Herkunftsland und die Herkunftsregion an.	1
IP-Set-Übereinstimmung	Gleicht die Anforderung mit einer Reihe von IP-Adressen und -Adressbereichen ab.	1 für die meisten Fälle. Wenn Sie die Anweisung so konfigurieren, dass sie einen Header mit weitergeleiteten IP-Adressen verwendet und eine Position im Header von angebenAny, erhöhen Sie die WCUs um 4.
Regelanweisung für Bezeichnungsübereinstimmung	Prüft die Anforderung für Bezeichnungen, die durch andere Regeln in derselben Web-ACL hinzugefügt wurden.	1

Übereinstimmungsanweisung	Beschreibung	WCUs
Regex-Übereinstimmungsregel-Anweisung	<p>Vergleicht ein Regex-Muster mit einer bestimmten Anforderungskomponente.</p>	<p>3, als Basiskosten.</p> <p>Wenn Sie die Anforderungskomponente All query parameters (Alle Abfrageparameter) verwenden, fügen Sie 10 WCUs hinzu. Wenn Sie die Anforderungskomponente JSON body (JSON-Text) verwenden, verdoppeln Sie die Basiskosten-WCUs. Für jede Texttransformation, die Sie anwenden, fügen Sie 10 WCUs hinzu.</p>
Regex-Mustersatz	<p>Vergleicht RegEx-Muster mit einer bestimmten Anforderungskomponente.</p>	<p>25 pro Mustersatz, als Basiskosten.</p> <p>Wenn Sie die Anforderungskomponente All query parameters (Alle Abfrageparameter) verwenden, fügen Sie 10 WCUs hinzu. Wenn Sie die Anforderungskomponente JSON body (JSON-Text) verwenden, verdoppeln Sie die Basiskosten-WCUs. Für jede Texttransformation, die Sie anwenden, fügen Sie 10 WCUs hinzu.</p>

Übereinstimmungsanweisung	Beschreibung	WCUs
Größenbeschränkung	Prüft Größenbeschränkungen gegen eine bestimmte Anforderungskomponente.	1, als Basiskosten. Wenn Sie die Anforderungskomponente All query parameters (Alle Abfrageparameter) verwenden, fügen Sie 10 WCUs hinzu. Wenn Sie die Anforderungskomponente JSON body (JSON-Text) verwenden, verdoppeln Sie die Basiskosten-WCUs. Für jede Texttransformation, die Sie anwenden, fügen Sie 10 WCUs hinzu.
SQLi-Angriff	Sucht nach schädlichem SQL-Code in einer bestimmten Anforderungskomponente.	20, als Basiskosten. Wenn Sie die Anforderungskomponente All query parameters (Alle Abfrageparameter) verwenden, fügen Sie 10 WCUs hinzu. Wenn Sie die Anforderungskomponente JSON body (JSON-Text) verwenden, verdoppeln Sie die Basiskosten-WCUs. Für jede Texttransformation, die Sie anwenden, fügen Sie 10 WCUs hinzu.

Übereinstimmungsanweisung	Beschreibung	WCUs
Zeichenfolgen-Übereinstimmung	<p>Vergleicht eine Zeichenfolge mit einer angegebenen Anforderungskomponente.</p>	<p>Die Basiskosten hängen vom Typ der Zeichenfolgen-Übereinstimmung ab und liegen zwischen 1 und 10.</p> <p>Wenn Sie die Anforderungskomponente All query parameters (Alle Abfrageparameter) verwenden, fügen Sie 10 WCUs hinzu. Wenn Sie die Anforderungskomponente JSON body (JSON-Text) verwenden, verdoppeln Sie die Basiskosten-WCUs. Für jede Texttransformation, die Sie anwenden, fügen Sie 10 WCUs hinzu.</p>
XSS-Scripting-Angriff	<p>Überprüft auf Cross-Site-Scripting-Angriffe in einer bestimmten Anforderungskomponente.</p>	<p>40, als Basiskosten.</p> <p>Wenn Sie die Anforderungskomponente All query parameters (Alle Abfrageparameter) verwenden, fügen Sie 10 WCUs hinzu. Wenn Sie die Anforderungskomponente JSON body (JSON-Text) verwenden, verdoppeln Sie die Basiskosten-WCUs. Für jede Texttransformation, die Sie anwenden, fügen Sie 10 WCUs hinzu.</p>

Anweisung für Regel zur geographischen Übereinstimmung

Verwenden Sie geografische Angaben oder Geo-Match-Angaben, um Webanfragen basierend auf dem Herkunftsland und der Herkunftsregion zu verwalten. Eine Geo-Match-Anweisung fügt Webanfragen Labels hinzu, die das Herkunftsland und die Herkunftsregion angeben. Diese Bezeichnungen werden unabhängig davon hinzugefügt, ob die Kriterien für die Aussage mit der Anfrage übereinstimmen. Eine Geo-Match-Anweisung führt auch einen Abgleich mit dem Herkunftsland der Anfrage durch.

Wie benutzt man die Geo-Match-Erklärung

Sie können die Geo-Match-Anweisung wie folgt für den Länder- oder Regionalabgleich verwenden:

- **Land** — Sie können eine Geo-Match-Regel als eigenständige Geo-Match-Regel verwenden, um Anfragen zu verwalten, die ausschließlich auf ihrem Herkunftsland basieren. Die Regelaussage stimmt mit den Ländercodes überein. Sie können auch einer Geo-Match-Regel mit einer Label-Match-Regel folgen, die mit dem Herkunftsland-Label übereinstimmt.
- **Region** — Verwenden Sie eine Geo-Match-Regel, gefolgt von einer Label-Match-Regel, um Anfragen auf der Grundlage ihrer Herkunftsregion zu verwalten. Sie können eine Geo-Match-Regel nicht allein für den Abgleich mit Regionscodes verwenden.

Informationen zur Verwendung von Label-Abgleichsregeln finden Sie unter [Regelanweisung für Bezeichnungsübereinstimmung](#) und [AWS WAF Labels auf Webanfragen](#).

So funktioniert die Geo-Match-Anweisung

AWS WAF Verwaltet mit der Geo-Match-Anweisung jede Webanfrage wie folgt:

1. **Ermittelt die Landes- und Regionalcodes der Anfrage** — AWS WAF bestimmt das Land und die Region einer Anfrage anhand ihrer IP-Adresse. AWS WAF Verwendet standardmäßig die IP-Adresse des Ursprungs der Webanfrage. Sie können anweisen AWS WAF , eine IP-Adresse aus einem alternativen Anforderungsheader zu verwenden `X-Forwarded-For`, indem Sie beispielsweise die Konfiguration für weitergeleitete IP-Adressen in den Einstellungen für die Regelanweisung aktivieren.

AWS WAF bestimmt den Speicherort von Anfragen mithilfe von MaxMind GeoIP-Datenbanken. MaxMind meldet eine sehr hohe Genauigkeit ihrer Daten auf Landesebene, obwohl die Genauigkeit je nach Faktoren wie Land und Art des geistigen Eigentums variiert. Weitere Informationen MaxMind dazu finden Sie unter [MaxMind IP-Geolokalisierung](#). Wenn Sie der

Meinung sind, dass einige der GeoIP-Daten falsch sind, können Sie unter [MaxMind Correct GeoIP2](#) Data eine Korrekturanfrage an Maxmind stellen.

AWS WAF verwendet die Alpha-2-Länder- und Regionscodes der Norm 3166 der Internationalen Organisation für Normung (ISO). Sie finden die Codes an den folgenden Stellen:

- Auf der ISO-Website können Sie auf der [ISO Online Browsing Platform \(OBP\)](#) nach den Ländercodes suchen.
- Auf Wikipedia sind die Ländercodes bei [ISO 3166-2](#) aufgeführt.

Die Regionalcodes für ein Land sind unter der URL aufgeführt. [https://en.wikipedia.org/wiki/ISO_3166-2:<ISO country code> Die Regionen für die Vereinigten Staaten entsprechen beispielsweise ISO 3166-2:US und für die Ukraine ISO 3166-2:UA](https://en.wikipedia.org/wiki/ISO_3166-2:<ISO_country_code>_Die_Regionen_für_die_Vereinigten_Staaten_entsprechen_beispielsweise_ISO_3166-2:US_und_für_die_Ukraine_ISO_3166-2:UA).

2. Bestimmt das Landes- und Regionslabel, das der Anfrage hinzugefügt werden soll — Die Beschriftungen geben an, ob die Geo-Match-Anweisung die Quell-IP oder eine weitergeleitete IP-Konfiguration verwendet.

- Herkunfts-IP

Das Länderlabel ist `aws:waf:clientip:geo:country:<ISO country code>`. Beispiel für die Vereinigten Staaten: `aws:waf:clientip:geo:country:US`.

Die Bezeichnung der Region lautet `aws:waf:clientip:geo:region:<ISO country code>-<ISO region code>`. Beispiel für Oregon in den Vereinigten Staaten: `aws:waf:clientip:geo:region:US-OR`.

- Weitergeleitete IP

Das Länderlabel ist `aws:waf:forwardedip:geo:country:<ISO country code>`. Beispiel für die Vereinigten Staaten: `aws:waf:forwardedip:geo:country:US`.

Die Bezeichnung der Region lautet `aws:waf:forwardedip:geo:region:<ISO country code>-<ISO region code>`. Beispiel für Oregon in den Vereinigten Staaten: `aws:waf:forwardedip:geo:region:US-OR`.

Wenn der Landes- oder Regionalcode für die angegebene IP-Adresse einer Anfrage nicht verfügbar ist, AWS WAF wird er XX in den Labels anstelle des Werts verwendet. Das folgende Label bezieht sich beispielsweise auf eine Client-IP, deren Landescode nicht verfügbar ist: `aws:waf:clientip:geo:country:XX` und das Folgende gilt für eine weitergeleitete

IP, deren Land die Vereinigten Staaten ist, deren Regionalcode jedoch nicht verfügbar
`ist:aws:waf:forwardedip:geo:region:US-XX`.

3. Prüft den Ländercode der Anfrage anhand der Regelkriterien

Die Geo-Match-Anweisung fügt allen Anfragen, die geprüft werden, Länder- und Regionskennzeichnungen hinzu, unabhängig davon, ob eine Übereinstimmung gefunden wird.

Note

AWS WAF fügt am Ende der Auswertung der Webanforderung einer Regel alle Bezeichnungen hinzu. Aus diesem Grund muss jeder Labelabgleich, den Sie mit den Beschriftungen aus einer Geo-Match-Anweisung verwenden, in einer anderen Regel definiert werden als die Regel, die die Geo-Match-Anweisung enthält.

Wenn Sie nur Regionswerte überprüfen möchten, können Sie eine Geo-Match-Regel mit Count Aktion und einer einzigen Übereinstimmung mit der Landesvorwahl schreiben, gefolgt von einer Label-Abgleichsregel für die Regions-Labels. Sie müssen einen Ländercode angeben, damit die Geo-Match-Regel ausgewertet werden kann, auch bei diesem Ansatz. Sie können die Anzahl von Protokollierungs- und Zählmetriken reduzieren, indem Sie ein Land angeben, von dem es sehr unwahrscheinlich ist, dass Besucher auf Ihre Website gelangen.

CloudFront Verteilungen und die Funktion zur CloudFront geografischen Beschränkung

Beachten Sie bei CloudFront Verteilungen, wenn Sie die CloudFront Funktion zur geografischen Beschränkung verwenden, dass die Funktion blockierte Anfragen nicht weiterleitet. AWS WAF Zulässige Anfragen werden weitergeleitet an AWS WAF. Wenn Sie Anfragen aufgrund der geografischen Lage und anderer Kriterien, die Sie angeben können, blockieren möchten AWS WAF, verwenden Sie die AWS WAF Geo-Match-Anweisung und nicht die Funktion zur CloudFront geografischen Beschränkung.

Eigenschaften der Geo-Match-Aussage

Verschachtelung – Sie können diesen Anweisungstyp verschachteln.

WCUs – 1 WCU.

Einstellungen — Diese Anweisung verwendet die folgenden Einstellungen:

- Ländercodes — Eine Reihe von Ländercodes, die für einen Geo-Match verglichen werden können. Dabei muss es sich um zweistellige Ländercodes aus den ISO-Alpha-2-Ländercodes der internationalen Norm ISO 3166 handeln, zum Beispiel. ["US", "CN"]
- (Optional) Konfiguration für weitergeleitete IP-Adressen — AWS WAF verwendet standardmäßig die IP-Adresse im Ursprung der Webanfrage, um das Herkunftsland zu ermitteln. Alternativ können Sie die Regel so konfigurieren, dass X-Forwarded-For stattdessen eine weitergeleitete IP in einem HTTP-Header verwendet wird. AWS WAF verwendet die erste IP-Adresse im Header. Mit dieser Konfiguration geben Sie auch ein Fallback-Verhalten an, das auf eine Webanfrage mit einer falsch formatierten IP-Adresse im Header angewendet wird. Das Fallback-Verhalten legt das Übereinstimmungsergebnis für die Anforderung fest, auf Übereinstimmung oder keine Übereinstimmung. Weitere Informationen finden Sie unter [Weitergeleitete IP-Adresse](#).

Wo finde ich diese Regelaussage

- Rule Builder in der Konsole – Wählen Sie für Request option (Anforderungsoption) die Option Originates from a country in (Ursprung aus einem Land in) aus.
- API — [GeoMatchStatement](#)

Beispiele

Sie können das Geo-Match-Statement verwenden, um Anfragen aus bestimmten Ländern oder Regionen zu verwalten. Wenn Sie beispielsweise Anfragen aus bestimmten Ländern blockieren möchten, aber dennoch Anfragen von einer bestimmten Gruppe von IP-Adressen in diesen Ländern zulassen möchten, könnten Sie eine Regel mit der Einstellung der Aktion auf Block und den folgenden verschachtelten Anweisungen erstellen, die in Pseudocode dargestellt werden:

- AND-Anweisung
 - Geomatch-Anweisung, die die Länder auflistet, die Sie blockieren möchten
 - NOT-Anweisung
 - IP-Set-Anweisung, die die IP-Adressen angibt, die Sie zulassen möchten.

Oder wenn Sie einige Regionen in bestimmten Ländern blockieren, aber dennoch Anfragen aus anderen Regionen in diesen Ländern zulassen möchten, können Sie zunächst eine Geo-Match-Regel definieren, bei der die Aktion auf eingestellt ist. Count Definieren Sie dann eine Label-Match-Regel, die mit den hinzugefügten Geo-Match-Labels übereinstimmt und die Anfragen nach Bedarf bearbeitet.

Der folgende Pseudocode beschreibt ein Beispiel für diesen Ansatz:

1. Geo-Match-Statement, in dem die Länder mit Regionen aufgeführt sind, die Sie blockieren möchten, deren Aktion jedoch auf Count gesetzt ist. Dadurch wird jede Webanfrage unabhängig vom Abgleichstatus gekennzeichnet und Sie erhalten außerdem Zählwerte für die Länder, für die Sie von Interesse sind.
2. ANDAnweisung mit Block-Aktion
 - Label Match-Anweisung, die die Labels für die Länder angibt, die Sie blockieren möchten
 - NOT-Anweisung
 - Label Match-Anweisung, die die Bezeichnungen der Regionen in den Ländern angibt, die Sie durchlassen möchten

Die folgende JSON-Liste zeigt eine Implementierung der beiden Regeln, die im vorherigen Pseudocode beschrieben wurden. Diese Regeln blockieren den gesamten Verkehr aus den Vereinigten Staaten mit Ausnahme des Verkehrs aus Oregon und Washington. In der Geo-Match-Anweisung werden allen Anfragen, die geprüft werden, Länder- und Regionsetiketten hinzugefügt. Die Label-Match-Regel wird nach der Geo-Match-Regel ausgeführt, sodass sie mit den Land- und Regionsbezeichnungen abgeglichen werden kann, die die Geo-Match-Regel gerade hinzugefügt hat. Die Geo-Match-Anweisung verwendet eine weitergeleitete IP-Adresse, sodass beim Labelabgleich auch weitergeleitete IP-Labels angegeben werden.

```
{
  "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": "awsfaf:forwardedip:geo:country:US"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "OrStatement": {
                "Statements": [
                  {
                    "LabelMatchStatement": {
                      "Scope": "LABEL",
                      "Key": "awsfaf:forwardedip:geo:region:US-OR"
                    }
                  },
                  {
                    "LabelMatchStatement": {
                      "Scope": "LABEL",
                      "Key": "awsfaf:forwardedip:geo:region:US-WA"
                    }
                  }
                ]
              }
            }
          }
        }
      ]
    }
  }
},
{
  "Action": {
    "Block": {}
  }
}
```

```

},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "blockUSButNotORorWA"
}
}

```

Als weiteres Beispiel können Sie Geo-Matching mit ratenbasierten Regeln kombinieren, um Ressourcen für Benutzer in einem bestimmten Land oder einer bestimmten Region zu priorisieren. Sie erstellen für jede Geo-Match- oder Label-Match-Aussage, die Sie zur Differenzierung Ihrer Benutzer verwenden, eine andere ratenbasierte Abrechnung. Legen Sie ein höheres Ratenlimit für Benutzer im bevorzugten Land oder der bevorzugten Region und ein niedrigeres Ratenlimit für andere Benutzer fest.

Die folgende JSON-Liste zeigt eine Geo-Match-Regel, gefolgt von ratenbasierten Regeln, die den Traffic aus den USA begrenzen. Die Regeln ermöglichen es, dass Verkehr aus Oregon mit einer höheren Rate eingetht als Verkehr aus anderen Teilen des Landes.

```

{
  "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": "awsfaf: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": "awsfaf:clientip:geo:country:US"
                }
              },
              {
                "NotStatement": {
                  "Statement": {
                    "LabelMatchStatement": {
                      "Scope": "LABEL",
                      "Key": "awsfaf:clientip:geo:region:US-OR"
                    }
                  }
                }
              }
            ]
          }
        }
      }
    }
  }
}

```

```
        }
      }
    ]
  }
}
},
"Action": {
  "Block": {}
},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "rateLimitUSNotOR"
}
}
```

IP-Set-Übereinstimmungsregelanweisung

Die IP-Set-Übereinstimmungsanweisung gleicht die IP-Adresse einer Webanforderung mit einer Reihe von IP-Adressen und -Adressbereichen ab. Verwenden Sie diese Option, um Webanforderungen basierend auf den IP-Adressen zuzulassen oder zu blockieren, von denen die Anforderungen stammen. Standardmäßig verwendet AWS WAF die IP-Adresse aus dem Ursprung der Webanforderung, aber Sie können die Regel so konfigurieren, dass sie einen HTTP-Header wie X-Forwarded-For verwendet.

AWS WAF unterstützt alle IPv4- und IPv6-CIDR-Bereiche außer `/0`. Weitere Informationen zur CIDR-Notation finden Sie im Wikipedia-Artikel [Classless Inter-Domain Routing](#). Ein IP-Set kann bis zu 10.000 IP-Adressen oder IP-Adressbereiche zur Überprüfung aufnehmen.

Note

Jede IP-Set-Match-Regel verweist auf ein IP-Set, das Sie unabhängig von Ihren Regeln erstellen und pflegen. Sie können einen einzelnen IP-Satz in mehreren Regeln verwenden. Wenn Sie den referenzierten Satz aktualisieren, AWS WAF werden automatisch alle Regeln aktualisiert, die darauf verweisen.

Informationen zum Erstellen und Verwalten eines IP-Sets finden Sie unter [Erstellen und verwalten eines IP-Sets](#).

Wenn Sie die Regeln in Ihrer Regelgruppe oder Web-ACL hinzufügen oder aktualisieren, wählen Sie die Option IP-Set und wählen Sie den Namen des IP-Sets, das Sie verwenden möchten.

Verschachtelung – Sie können diesen Anweisungstyp verschachteln.

WCUs – 1 WCU für die meisten. Wenn Sie die Anweisung für die Verwendung weitergeleiteter IP-Adressen konfigurieren und eine Position von angebenANY, erhöhen Sie die WCU-Nutzung um 4.

Diese Anweisung verwendet die folgenden Einstellungen:

- IP-Set-Spezifikation – Wählen Sie in der Liste das IP-Set, das Sie verwenden möchten, oder erstellen Sie ein neues.
- (Optional) Weitergeleitete IP-Konfiguration – ein alternativer weitergeleiteter IP-Header-Name, der anstelle des Anforderungsursprungs verwendet werden soll. Sie geben an, ob ein Abgleich mit der ersten, letzten oder irgendeiner Adresse im Header durchgeführt werden soll. Außerdem geben Sie ein Fallback-Verhalten an, das auf eine Webanforderung mit einer fehlerhaften IP-Adresse im angegebenen Header angewendet werden soll. Das Fallback-Verhalten legt das Übereinstimmungsergebnis für die Anforderung fest, auf Übereinstimmung oder keine Übereinstimmung. Weitere Informationen finden Sie unter [Weitergeleitete IP-Adresse](#).

Wo finde ich diese Regelaussage


- Rule Builder in der Konsole – Wählen Sie für Request option (Anforderungsoption) die Option Originates from an IP address in (Ursprung von einer IP-Adresse in) aus.
- Seite Add my own rules and rule groups (Eigene Regeln und Regelgruppen hinzufügen) in der Konsole. Wählen Sie die Option IP set (IP-Set) aus.
- API — [IP SetReferenceStatement](#)

Regelanweisung für Bezeichnungsübereinstimmung

Die Bezeichnungs-Übereinstimmungsanweisung gleicht die Bezeichnungen, die sich in der Webanforderung befinden, mit einer Zeichenfolgenspezifikation ab. Die Bezeichnungen, die einer Regel zur Überprüfung zur Verfügung stehen, sind diejenigen, die der Webanforderung bereits durch andere Regeln in derselben Web-ACL-Auswertung hinzugefügt wurden.

Labels bleiben außerhalb der Web-ACL-Auswertung nicht erhalten, aber Sie können auf Label-Metriken zugreifen CloudWatch und in der Konsole Zusammenfassungen der Labelinformationen für jede Web-ACL einsehen. AWS WAF Weitere Informationen finden Sie unter [Kennzeichen](#)

[Sie Metriken und Dimensionen](#) und [Überwachung und Tuning](#). Sie können Labels auch in den Protokollen sehen. Weitere Informationen finden Sie unter [Protokollfelder](#).

 Note

Eine Bezeichnungs-Übereinstimmungsanweisung kann nur Bezeichnungen von Regeln sehen, die zuvor in der Web-ACL ausgewertet wurden. Informationen darüber, wie die Regeln und Regelgruppen in einer Web-ACL AWS WAF ausgewertet werden, finden Sie unter [Reihenfolge der Verarbeitung von Regeln und Regelgruppen in einer Web-ACL](#).

Weitere Informationen zum Hinzufügen und Abgleichen von Labels finden Sie unter [AWS WAF Labels auf Webanfragen](#).

Verschachtelung – Sie können diesen Anweisungstyp verschachteln.

WCUs – 1 WCU

Diese Anweisung verwendet die folgenden Einstellungen:

- **Übereinstimmungsumfang** – Setzen Sie das auf Label (Bezeichnung), um einen Abgleich mit dem Bezeichnungsnamen und optional den vorhergehenden Namespaces und dem vorhergehenden Präfix durchzuführen. Stellen Sie das auf Namespace, um einen Abgleich mit einigen oder allen Namespace-Spezifikationen und optional dem vorhergehenden Präfix durchzuführen.
- **Schlüssel** – Die Zeichenfolge, mit der Sie einen Abgleich durchführen möchten. Wenn Sie einen Namespace-Übereinstimmungsumfang angeben, sollten Sie nur Namespaces und optional das Präfix mit einem abschließenden Doppelpunkt angeben. Wenn Sie einen Bezeichnungs-Übereinstimmungsbereich angeben, muss dieser den Namen der Bezeichnung enthalten und kann optional vorhergehende Namespaces und das vorhergehende Präfix enthalten.

Weitere Informationen zu diesen Einstellungen finden Sie unter [Abgleich mit einer Bezeichnung](#) und [Beispiele für Bezeichnungsabgleich](#).

Wo finde ich diese Regelaussage

- Rule Builder in der Konsole – Wählen Sie für Request option (Anforderungsoption) die Option Has label (Hat Bezeichnung) aus.
- API — [LabelMatchStatement](#)

Regex-Übereinstimmungsregel-Anweisung

Eine Regex-Match-Anweisung weist AWS WAF an, eine Anforderungskomponente mit einem einzigen regulären Ausdruck (Regex) abzugleichen. Eine Webanforderung stimmt mit der Anweisung überein, wenn die Anforderungskomponente mit dem angegebenen regulären Ausdruck übereinstimmt.

Dieser Anweisungstyp ist eine gute Alternative zu [Regex-Mustersatz Übereinstimmungsregelanweisung](#) für Situationen, in denen Sie Ihre Übereinstimmungskriterien mit mathematischer Logik kombinieren möchten. Wenn Sie beispielsweise möchten, dass eine Anforderungskomponente einen Abgleich mit einigen regulären Ausdrücken vornimmt, aber andere ausschließt, können Sie die Regex-Übereinstimmungsanweisungen mit [AND-Regelanweisung](#) und [NOT-Regelanweisung](#) kombinieren.

AWS WAF unterstützt mit einigen Ausnahmen die von der PCRE-Bibliothek verwendete Mustersyntax. `libpcre` Die Bibliothek ist unter [PCRE - Perl Compatible Regular Expressions](#) (Perl-kompatible reguläre Ausdrücke) dokumentiert. Hinweise zur AWS WAF Unterstützung finden Sie unter [Musterabgleich mit regulären Ausdrücken in AWS WAF](#).

Verschachtelung – Sie können diesen Anweisungstyp verschachteln.

WCUs – 3 WCUs als Basiskosten. Wenn Sie die Anforderungskomponente All query parameters (Alle Abfrageparameter) verwenden, fügen Sie 10 WCUs hinzu. Wenn Sie die Anforderungskomponente JSON body (JSON-Text) verwenden, verdoppeln Sie die Basiskosten-WCUs. Für jede Texttransformation, die Sie anwenden, fügen Sie 10 WCUs hinzu.

Dieser Anweisungstyp arbeitet mit einer Webanforderungskomponente und erfordert die folgenden Einstellungen für Anforderungskomponenten:

- Anforderungskomponente — Der Teil der Webanforderung, der überprüft werden soll, z. B. eine Abfragezeichenfolge oder der Hauptteil.

Warning

Wenn Sie die Anforderungskomponenten Body, JSON-Text, Header oder Cookies untersuchen, sollten Sie sich über die Einschränkungen informieren, mit denen der Inhalt überprüft AWS WAF werden kann. [Umgang mit übergroßen Webanforderungskomponenten in AWS WAF](#)

Informationen über Webanforderungskomponenten finden Sie unter [Webanforderungskomponenten](#).

- Optionale Texttransformationen — Transformationen, die Sie an der Anforderungskomponente durchführen AWS WAF möchten, bevor Sie sie überprüfen. Sie könnten beispielsweise in Kleinschreibung umwandeln oder Leerzeichen normalisieren. Wenn Sie mehr als eine Transformation angeben, werden diese in der angegebenen Reihenfolge AWS WAF verarbeitet. Weitere Informationen finden Sie unter [Texttransformationen](#).

Wo finde ich diese Regelaussage

- Rule Builder in der Konsole – Wählen Sie für Match type (Übereinstimmungstyp) die Option Matches regular expression (Stimmt mit regulärem Ausdruck überein) aus.
- API — [RegexMatchStatement](#)

Regex-Mustersatz Übereinstimmungsregelanweisung

Die Regex-Mustersatzübereinstimmung überprüft den Teil der Webanforderung, den Sie für die regulären Ausdrucksmuster angeben, die Sie in einem Regex-Mustersatz angegeben haben.

AWS WAF unterstützt die von der PCRE-Bibliothek verwendete Mustersyntax `libpcre` mit einigen Ausnahmen. Die Bibliothek ist unter [PCRE - Perl Compatible Regular Expressions](#) (Perl-kompatible reguläre Ausdrücke) dokumentiert. Hinweise zur AWS WAF Unterstützung finden Sie unter [Musterabgleich mit regulären Ausdrücken in AWS WAF](#).

Note

Jeder RegEx-Mustersatz bezieht sich auf einen RegEx-Mustersatz, den Sie unabhängig von Ihren Regeln erstellen und pflegen. Sie können einen einzelnen Regex-Mustersatz in mehreren Regeln verwenden. Wenn Sie den Satz aktualisieren, auf den verwiesen AWS WAF wird, werden automatisch alle Regeln aktualisiert, die darauf verweisen. Informationen zum Erstellen und Verwalten eines Regex-Mustersatzes finden Sie unter [Erstellen und Verwalten eines Regex-Mustersatzes](#).

Eine Regex-Patternset-Match-Anweisung weist AWS WAF an, innerhalb der von Ihnen ausgewählten Anforderungskomponente nach einem der Muster im Satz zu suchen. Eine Webanforderung stimmt

mit der Regelanweisung für den Mustersatz überein, wenn die Anforderungskomponente mit einem der Muster im Satz übereinstimmt.


Wenn Sie Ihre Regex-Musterabgleiche mit Logik kombinieren möchten, um beispielsweise einen Abgleich mit einigen regulären Ausdrücken vorzunehmen, aber andere auszuschließen, können Sie [Regex-Übereinstimmungsregel-Anweisung](#) verwenden.

Verschachtelung – Sie können diesen Anweisungstyp verschachteln.

WCUs — 25 WCUs als Basiskosten. Wenn Sie die Anforderungskomponente All query parameters (Alle Abfrageparameter) verwenden, fügen Sie 10 WCUs hinzu. Wenn Sie die Anforderungskomponente JSON body (JSON-Text) verwenden, verdoppeln Sie die Basiskosten-WCUs. Für jede Texttransformation, die Sie anwenden, fügen Sie 10 WCUs hinzu.

Dieser Anweisungstyp arbeitet mit einer Webanforderungskomponente und erfordert die folgenden Einstellungen für Anforderungskomponenten:

- Anforderungskomponente — Der Teil der Webanforderung, der überprüft werden soll, z. B. eine Abfragezeichenfolge oder der Hauptteil.

 Warning

Wenn Sie die Anforderungskomponenten Body, JSON-Text, Header oder Cookies untersuchen, sollten Sie sich über die Einschränkungen informieren, mit denen der Inhalt überprüft AWS WAF werden kann. [Umgang mit übergroßen Webanforderungskomponenten in AWS WAF](#)

Informationen über Webanforderungskomponenten finden Sie unter [Webanforderungskomponenten](#).

- Optionale Texttransformationen — Transformationen, die Sie an der Anforderungskomponente durchführen AWS WAF möchten, bevor Sie sie überprüfen. Sie könnten beispielsweise in Kleinschreibung umwandeln oder Leerzeichen normalisieren. Wenn Sie mehr als eine Transformation angeben, werden diese in der angegebenen Reihenfolge AWS WAF verarbeitet. Weitere Informationen finden Sie unter [Texttransformationen](#).

Diese Anweisung erfordert die folgenden Einstellungen:

- **Regex-Mustersatz-Spezifikation** – Wählen Sie aus der Liste den Regex-Mustersatz, den Sie verwenden möchten, oder erstellen Sie einen neuen.

Wo finde ich diese Regelaussage

- **Rule Builder in der Konsole** – Wählen Sie für Match type (Übereinstimmungstyp) die Option String Match Condition (Zeichenfolgen-Übereinstimmungsbedingungen) > Matches pattern from regular expression set (Muster aus dem Satz mit regulärem Ausdruck stimmt überein) aus.
- **API** — [RegexPatternSetReferenceStatement](#)

Größenbeschränkungsanweisung

Eine Größenbeschränkungsanweisung vergleicht die Anzahl der Byte in einer Webanforderungskomponente mit einer von Ihnen angegebenen Zahl und entspricht Ihren Vergleichskriterien. Das Vergleichskriterium ist ein Operator wie größer als (>) oder kleiner als (<). Sie können beispielsweise Anfragen mit einer Abfragezeichenfolge mit einer Größe von mehr als 100 Byte abgleichen.

Note

Diese Anweisung überprüft nur die Größe der Webanforderungskomponente. Sie überprüft nicht den Inhalt der Komponente.

Wenn Sie den URI-Pfad überprüfen, zählt jeder Eintrag / im Pfad als ein Zeichen. Der URI-Pfad / Logo.jpg ist beispielsweise neun Zeichen lang.

Verschachtelung – Sie können diesen Anweisungstyp verschachteln.

WCUs – 1 WCU als Basiskosten. Wenn Sie die Anforderungskomponente All query parameters (Alle Abfrageparameter) verwenden, fügen Sie 10 WCUs hinzu. Wenn Sie die Anforderungskomponente JSON body (JSON-Text) verwenden, verdoppeln Sie die Basiskosten-WCUs. Für jede Texttransformation, die Sie anwenden, fügen Sie 10 WCUs hinzu.

Dieser Anweisungstyp arbeitet mit einer Webanforderungskomponente und erfordert die folgenden Einstellungen für Anforderungskomponenten:

- **Anforderungskomponente** — Der Teil der Webanforderung, der überprüft werden soll, z. B. eine Abfragezeichenfolge oder der Hauptteil. Informationen über Webanforderungskomponenten finden Sie unter [Webanforderungskomponenten](#).

Eine Größenbeschränkungsanweisung überprüft nur die Größe der Komponente, nachdem alle Transformationen angewendet wurden. Sie überprüft nicht den Inhalt der Komponente.

- **Optionale Texttransformationen** — Transformationen, die Sie AWS WAF an der Anforderungskomponente durchführen möchten, bevor Sie deren Größe überprüfen. Sie könnten beispielsweise Leerraum komprimieren oder HTML-Entitäten dekodieren. Wenn Sie mehr als eine Transformation angeben, AWS WAF werden diese in der angegebenen Reihenfolge verarbeitet. Weitere Informationen finden Sie unter [Texttransformationen](#).

Zusätzlich erfordert diese Anweisung die folgenden Einstellungen:

- **Größenabgleichsbedingung** – Dies gibt den numerischen Vergleichsoperator an, der verwendet werden soll, um die angegebene Größe mit der von Ihnen gewählten Anforderungskomponente zu vergleichen. Wählen Sie den Operator aus der Liste aus.
- **Größe** — Die Größeneinstellung in Byte, die für den Vergleich verwendet werden soll.

Wo finde ich diese Regelaussage

- **Rule Builder in der Konsole** – Wählen Sie für Match type (Übereinstimmungstyp) unter Size Match Condition (Größen-Übereinstimmungsbedingung) die Bedingung aus, die Sie verwenden möchten.
- **API** — [SizeConstraintStatement](#)

SQL-Injection-Angriff-Regelanweisung

Eine SQL-Injection-Regelanweisung sucht nach böartigem SQL-Code. Angreifer fügen böartigen SQL-Code in Webanfragen ein, um beispielsweise Ihre Datenbank zu ändern oder Daten daraus zu extrahieren.

Verschachtelung – Sie können diesen Anweisungstyp verschachteln.


WCUs — Die Grundkosten hängen von der Einstellung der Sensitivitätsstufe für die Regelaussage ab: Low Kosten 20 und High Kosten 30.

Wenn Sie die Anforderungskomponente All query parameters (Alle Abfrageparameter) verwenden, fügen Sie 10 WCUs hinzu. Wenn Sie die Anforderungskomponente JSON body (JSON-Text)

verwenden, verdoppeln Sie die Basiskosten-WCUs. Für jede Texttransformation, die Sie anwenden, fügen Sie 10 WCUs hinzu.

Dieser Anweisungstyp arbeitet mit einer Webanforderungskomponente und erfordert die folgenden Einstellungen für Anforderungskomponenten:

- **Anforderungskomponente** — Der Teil der Webanforderung, der überprüft werden soll, z. B. eine Abfragezeichenfolge oder der Hauptteil.

 **Warning**

Wenn Sie die Anforderungskomponenten Body, JSON-Text, Header oder Cookies untersuchen, sollten Sie sich über die Einschränkungen informieren, mit denen der Inhalt überprüft AWS WAF werden kann. [Umgang mit übergroßen Webanforderungskomponenten in AWS WAF](#)

Informationen über Webanforderungskomponenten finden Sie unter [Webanforderungskomponenten](#).

- **Optionale Texttransformationen** — Transformationen, die Sie an der Anforderungskomponente durchführen AWS WAF möchten, bevor Sie sie überprüfen. Sie könnten beispielsweise in Kleinschreibung umwandeln oder Leerzeichen normalisieren. Wenn Sie mehr als eine Transformation angeben, werden diese in der angegebenen Reihenfolge AWS WAF verarbeitet. Weitere Informationen finden Sie unter [Texttransformationen](#).

Darüber hinaus erfordert diese Anweisung die folgende Einstellung:

- **Sensitivitätsstufe** — Mit dieser Einstellung wird die Sensitivität der SQL-Injection-Übereinstimmungskriterien eingestellt. Die Optionen sind LOW und HIGH. Die Standardeinstellung lautet LOW.

Diese HIGH Einstellung erkennt mehr SQL-Injection-Angriffe und ist die empfohlene Einstellung. Aufgrund der höheren Empfindlichkeit generiert diese Einstellung mehr Fehlalarme, insbesondere wenn Ihre Webanfragen normalerweise ungewöhnliche Zeichenfolgen enthalten. Beim Testen und Optimieren Ihrer Web-ACLs müssen Sie möglicherweise mehr tun, um Fehlalarme zu vermeiden. Weitere Informationen finden Sie unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

Die niedrigere Einstellung ermöglicht eine weniger strenge Erkennung von SQL-Injections, was auch zu weniger Fehlalarmen führt. LOW kann eine bessere Wahl für Ressourcen sein, die über andere Schutzmaßnahmen gegen SQL-Injection-Angriffe verfügen oder die eine geringe Toleranz gegenüber Fehlalarmen aufweisen.

Wo finde ich diese Regelaussage

- Rule Builder in der Konsole – Wählen Sie für Match type (Übereinstimmungstyp) die Option Attack match conditions (Bedingungen für Angriffsabgleich) > Contains SQL injection attacks (Enthält SQL-Injection-Angriffe) aus.
- API — [SqliMatchStatement](#)

Zeichenfolgen-Übereinstimmungsanweisung

Eine String-Match-Anweisung gibt an, AWS WAF nach welcher Zeichenfolge Sie in einer Anfrage suchen möchten, wo in der Anfrage gesucht werden soll und wie. Beispielsweise können Sie nach einer bestimmten Zeichenfolge am Anfang einer beliebigen Suchzeichenfolge in der Anforderung oder als genaue Übereinstimmung mit dem User-agent-Header der Anforderung suchen. Normalerweise besteht die Zeichenfolge aus druckbaren ASCII-Zeichen, aber Sie können jedes beliebige Zeichen von hexadezimal 0x00 bis 0xFF (dezimal 0 bis 255) verwenden.

Verschachtelung – Sie können diesen Anweisungstyp verschachteln.


WCUs – Die Basiskosten sind abhängig von der Art der Übereinstimmung, die Sie verwenden.

- Stimmt genau mit Zeichenfolge überein – 2
- Beginnt mit Zeichenfolge – 2
- Endet mit Zeichenfolge – 2
- Enthält Zeichenfolge – 10
- Enthält das Wort — 10

Wenn Sie die Anforderungskomponente All query parameters (Alle Abfrageparameter) verwenden, fügen Sie 10 WCUs hinzu. Wenn Sie die Anforderungskomponente JSON body (JSON-Text) verwenden, verdoppeln Sie die Basiskosten-WCUs. Für jede Texttransformation, die Sie anwenden, fügen Sie 10 WCUs hinzu.

Dieser Anweisungstyp arbeitet mit einer Webanforderungskomponente und erfordert die folgenden Einstellungen für Anforderungskomponenten:

- Anforderungskomponente — Der Teil der Webanforderung, der untersucht werden soll, z. B. eine Abfragezeichenfolge oder der Hauptteil.

 Warning

Wenn Sie die Anforderungskomponenten Body, JSON-Text, Header oder Cookies untersuchen, sollten Sie sich über die Einschränkungen informieren, mit denen der Inhalt überprüft AWS WAF werden kann. [Umgang mit übergroßen Webanforderungskomponenten in AWS WAF](#)

Informationen über Webanforderungskomponenten finden Sie unter [Webanforderungskomponenten](#).

- Optionale Texttransformationen — Transformationen, die Sie an der Anforderungskomponente durchführen AWS WAF möchten, bevor Sie sie überprüfen. Sie könnten beispielsweise in Kleinschreibung umwandeln oder Leerzeichen normalisieren. Wenn Sie mehr als eine Transformation angeben, werden diese in der angegebenen Reihenfolge AWS WAF verarbeitet. Weitere Informationen finden Sie unter [Texttransformationen](#).

Zusätzlich erfordert diese Anweisung die folgenden Einstellungen:

- Übereinstimmende Zeichenfolge — Dies ist die Zeichenfolge, die Sie AWS WAF mit der angegebenen Anforderungskomponente vergleichen möchten. Normalerweise besteht die Zeichenfolge aus druckbaren ASCII-Zeichen, aber Sie können jedes beliebige Zeichen von hexadezimal 0x00 bis 0xFF (dezimal 0 bis 255) verwenden.
- Bedingung für übereinstimmende Zeichenfolge — Dies gibt den Suchtyp an, den Sie ausführen AWS WAF möchten.
 - Exactly matches string (Entspricht Zeichenfolge genau) – Die Zeichenfolge und der Wert der Steuerungskomponente sind identisch.
 - Starts with string (Beginnt mit Zeichenfolge) – Die Zeichenfolge wird am Anfang der Anforderungskomponente angezeigt.
 - Ends with string (Endet mit Zeichenfolge) – Die Zeichenfolge wird am Ende der Anforderungskomponente angezeigt.

- Contains string (Enthält Zeichenfolge) – Die Zeichenfolge wird an beliebiger Stelle in der Anforderungskomponente angezeigt.
- Contains word (Enthält Wort) – Die von Ihnen angegebene Zeichenfolge muss in der Anforderungskomponente angezeigt werden. Bei dieser Option darf die von Ihnen angegebene Zeichenfolge nur alphanumerische Zeichen oder Unterstriche (A-Z, a-z, 0-9 oder _) enthalten.

Eine der folgenden Bedingungen muss erfüllt sein, damit die Anforderung übereinstimmt:

- Die Zeichenfolge entspricht exakt dem Wert der Anforderungskomponente, z. B. dem Wert eines Headers.
- Die Zeichenfolge steht am Anfang der Anforderungskomponente und wird von einem anderen Zeichen als einem alphanumerischen Zeichen oder Unterstrich () gefolgt, z. B. BadBot ; .
- Die Zeichenfolge befindet sich am Ende der Anforderungskomponente und wird von einem anderen Zeichen als einem alphanumerischen Zeichen oder Unterstrich (), z. B. ;BadBot, eingeleitet.
- Die Zeichenfolge befindet sich in der Mitte der Anforderungskomponente und wird von anderen Zeichen als alphanumerischen Zeichen oder Unterstrichen () eingeleitet und gefolgt, z. B. - BadBot ; .

Wo finde ich diese Regelaussage

- Rule Builder in der Konsole – Wählen Sie für Match type (Übereinstimmungstyp) die Option String Match Condition (Zeichenfolgen-Übereinstimmungsbedingungen) aus. Geben Sie dann die Zeichenfolgen ein, mit denen Sie einen Vergleich vornehmen möchten.
- API — [ByteMatchStatement](#)

Cross-Site-Scripting-Angriffsregel-Anweisung

Eine XSS-Angriffsanweisung (Cross-Site Scripting) untersucht eine Webanforderungskomponente auf schädliche Skripts. Bei einem XSS-Angriff nutzt der Angreifer Sicherheitslücken auf einer harmlosen Website, um bösartige Client-Site-Skripts in andere legitime Webbrowser einzuschleusen.

Verschachtelung – Sie können diesen Anweisungstyp verschachteln.

WCUs – 40 WCUs als Basiskosten. Wenn Sie die Anforderungskomponente All query parameters (Alle Abfrageparameter) verwenden, fügen Sie 10 WCUs hinzu. Wenn Sie die

Anforderungskomponente JSON body (JSON-Text) verwenden, verdoppeln Sie die Basiskosten-WCUs. Für jede Texttransformation, die Sie anwenden, fügen Sie 10 WCUs hinzu.

Dieser Anweisungstyp arbeitet mit einer Webanforderungskomponente und erfordert die folgenden Einstellungen für Anforderungskomponenten:

- Anforderungskomponente — Der Teil der Webanfrage, der überprüft werden soll, z. B. eine Abfragezeichenfolge oder der Hauptteil.

Warning

Wenn Sie die Anforderungskomponenten Body, JSON-Text, Header oder Cookies untersuchen, sollten Sie sich über die Einschränkungen informieren, mit denen der Inhalt überprüft AWS WAF werden kann. [Umgang mit übergroßen Webanforderungskomponenten in AWS WAF](#)

Informationen über Webanforderungskomponenten finden Sie unter [Webanforderungskomponenten](#).

- Optionale Texttransformationen — Transformationen, die Sie an der Anforderungskomponente durchführen AWS WAF möchten, bevor Sie sie überprüfen. Sie könnten beispielsweise in Kleinschreibung umwandeln oder Leerzeichen normalisieren. Wenn Sie mehr als eine Transformation angeben, werden diese in der angegebenen Reihenfolge AWS WAF verarbeitet. Weitere Informationen finden Sie unter [Texttransformationen](#).

Wo finde ich diese Regelaussage

- Rule Builder in der Konsole – Wählen Sie für Match type (Übereinstimmungstyp) die Option Attack match conditions (Bedingungen für Angriffsabgleich) > Contains XSS injection attacks (Enthält XSS-Injection-Angriffe) aus.
- API — [XssMatchStatement](#)

Logische Regelaussagen

Verwenden Sie Anweisungen nach logischen Regeln, um andere Anweisungen zu kombinieren oder deren Ergebnisse zu negieren. Jede logische Regelanweisung benötigt mindestens eine verschachtelte Anweisung.

Verschachteln Sie die Anweisungen unter logischen Regelanweisungen, um die Ergebnisse der Regelanweisung logisch zu kombinieren oder zu negieren.

Logische Regelanweisungen sind verschachtelbar. Sie können sie in andere logische Regelanweisungen verschachteln und in Eingrenzungsanweisungen verwenden. Informationen zu Eingrenzungsanweisungen finden Sie unter [Eingrenzungsanweisungen](#).

Note

Der visuelle Editor in der Konsole unterstützt eine Ebene der Verschachtelung von Regelanweisungen, die für viele Anforderungen geeignet ist. Bearbeiten Sie die JSON-Darstellung der Regel in der Konsole oder verwenden Sie die APIs, um weitere Ebenen zu verschachteln.

In dieser Tabelle werden die Anweisungen für logische Regeln beschrieben und Richtlinien für die Berechnung der jeweiligen Nutzung von Web-ACL-Kapazitätseinheiten (WCU) bereitgestellt. Informationen zu den WCUs finden Sie unter [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#).

Logische Anweisung	Beschreibung	WCUs
AND-Logik	Kombiniert verschachtelte Anweisungen mit AND-Logik.	Basierend auf verschachtelten Anweisungen
NOT-Logik	Negiert die Ergebnisse einer verschachtelten Anweisung.	Basierend auf einer verschachtelten Anweisung
OR-Logik	Kombiniert verschachtelte Anweisungen mit OR-Logik.	Basierend auf verschachtelten Anweisungen

AND-Regelanweisung

Die AND-Regelanweisung kombiniert verschachtelte Anweisungen mit einer logischen AND-Verknüpfung, sodass alle verschachtelten Anweisungen übereinstimmen müssen, damit die AND-Anweisung übereinstimmt. Dies erfordert mindestens eine verschachtelte Anweisung.

Verschachtelung – Sie können diesen Anweisungstyp verschachteln.

WCUs – Abhängig von den verschachtelten Anweisungen.

Wo finde ich diese Regelerklärung

- Rule Builder in der Konsole – Wählen Sie für If a request (Wenn eine Anforderung) die Option matches all the statements (AND) (mit allen Anweisungen übereinstimmt (AND)) aus und füllen Sie dann die verschachtelten Anweisungen aus.
- API — [AndStatement](#)

Beispiele

Die folgende Liste zeigt die Verwendung von AND und NOT logische Regelanweisungen, um Fehlalarme aus den Treffern einer SQL-Injection-Angriffsanweisung zu eliminieren. Nehmen wir für dieses Beispiel an, dass wir eine Einzelbyte-Match-Anweisung schreiben können, um die Anfragen abzugleichen, die zu falsch positiven Ergebnissen führen.

Die AND-Anweisung stimmt für Anfragen überein, die nicht mit der Byte-Match-Anweisung übereinstimmen und die der SQL-Injection-Angriffsanweisung entsprechen.

```
{
  "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"
}
}
}

```

Mit dem visuellen Editor für Konsolenregeln können Sie eine unlogische Anweisung oder eine Anweisung unter einer NOT OR Oder-Anweisung verschachteln. AND Die Verschachtelung der NOT Anweisung ist im vorherigen Beispiel dargestellt.

Mit dem visuellen Editor für Konsolenregeln können Sie die meisten verschachtelbaren Anweisungen unter einer logischen Regelanweisung verschachteln, wie sie im vorherigen Beispiel gezeigt wurde. Sie können den Visual Editor nicht verwenden, um AND OD-Anweisungen zu verschachtelnOR. Um diese Art der Verschachtelung zu konfigurieren, müssen Sie Ihre Regelanweisung in JSON angeben. Die folgende JSON-Regelliste enthält beispielsweise eine Anweisung, die in einer OR Anweisung verschachtelt istAND.

```
{
  "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"
}
}
```

NOT-Regelanweisung

Die NOT-Regelanweisung negiert logisch die Ergebnisse einer einzelnen verschachtelten Anweisung, sodass die verschachtelten Anweisungen nicht mit der NOT-Anweisung übereinstimmen dürfen und umgekehrt. Dies erfordert eine verschachtelte Anweisung.

Wenn Sie beispielsweise Anforderungen blockieren möchten, die nicht aus einem bestimmten Land stammen, erstellen Sie eine NOT-Anweisung mit einer Aktion, die auf Blockieren festgelegt ist, und verschachteln Sie eine geografische Match-Anweisung, die das Land angibt.

Verschachtelung – Sie können diesen Anweisungstyp verschachteln.

WCUs – Abhängig von der verschachtelten Anweisung.

Wo finde ich diese Regelerklärung

- Rule Builder in der Konsole – Wählen Sie für If a request (Wenn eine Anforderung) die Option doesn't match the statement (NOT) (nicht mit der Anweisung übereinstimmt (NOT)) aus. Füllen Sie dann die verschachtelte Anweisung aus.
- API — [NotStatement](#)

OR-Regelanweisung

Die OR-Regelanweisung kombiniert verschachtelte Anweisungen mit der OR-Logik, sodass eine der verschachtelten Anweisungen übereinstimmen muss, damit die OR-Anweisung übereinstimmt. Dies erfordert mindestens eine verschachtelte Anweisung.

Wenn Sie beispielsweise Anfragen blockieren möchten, die aus einem bestimmten Land kommen oder eine bestimmte Abfragezeichenfolge enthalten, können Sie eine Anweisung erstellen und darin eine OR Geo-Match-Anweisung für das Land und eine String-Match-Anweisung für die Abfragezeichenfolge verschachteln.

Wenn Sie stattdessen Anfragen blockieren möchten, die nicht aus einem bestimmten Land stammen oder eine bestimmte Abfragezeichenfolge enthalten, würden Sie die vorherige OR Anweisung so ändern, dass die Geo-Match-Anweisung eine Ebene tiefer in einer NOT Anweisung verschachtelt wird. Diese Verschachtelungsebene erfordert die Verwendung der JSON-Formatierung, weil die Konsole nur eine Verschachtelungsebene unterstützt.

Verschachtelung – Sie können diesen Anweisungstyp verschachteln.

WCUs – Abhängig von den verschachtelten Anweisungen.

Wo finde ich diese Regelaussage

- Rule Builder in der Konsole – Wählen Sie für If a request (Wenn eine Anforderung) die Option matches at least one of the statements (OR) (mit mindestens einer der Anweisungen übereinstimmt (OR)) aus. Füllen Sie dann die verschachtelten Anweisungen aus.
- API — [OrStatement](#)

Beispiele

Die folgende Liste zeigt die Verwendung von OR, um zwei andere Anweisungen zu kombinieren. Die OR Anweisung ist eine Übereinstimmung, wenn eine der verschachtelten Anweisungen übereinstimmt.

```
{
  "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"
          }
        }
      ]
    }
  }
}

```

Mit dem visuellen Editor für Konsolenregeln können Sie die meisten verschachtelbaren Anweisungen unter einer logischen Regelanweisung verschachteln, aber Sie können den visuellen Editor nicht verwenden, um OR-Anweisungen zu verschachteln. Um diese Art der Verschachtelung zu konfigurieren, müssen Sie Ihre Regelanweisung in JSON angeben. Die folgende JSON-Regelliste enthält beispielsweise eine Anweisung, die in einer OR-Anweisung verschachtelt ist.

```

{
  "Name": "match_rule",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "aws:waf: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"  
}  
}
```

Ratenbasierte Regelanweisung

Eine ratenbasierte Regel zählt eingehende Anfragen und begrenzt die Rate der Anfragen, wenn sie zu schnell eingehen. Die Regel aggregiert Anfragen gemäß Ihren Kriterien und zählt und begrenzt die aggregierten Gruppierungen auf der Grundlage des Bewertungsfensters, des Anforderungslimits und der Aktionseinstellungen der Regel.

Note

Sie können Webanfragen auch mit der gezielten Schutzstufe der Regelgruppe „AWS Managed Rules“ von Bot Control einschränken. Für die Verwendung dieser verwalteten Regelgruppe fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter [Optionen zur Ratenbegrenzung in ratenbasierten Regeln und gezielten Bot-Kontrollregeln](#).

AWS WAF verfolgt und verwaltet Webanfragen separat für jede Instanz einer ratenbasierten Regel, die Sie verwenden. Wenn Sie beispielsweise dieselben ratenbasierten Regeleinstellungen in zwei Web-ACLs angeben, stellt jede der beiden Regelanweisungen eine separate Instanz der ratenbasierten Regel dar und jede erhält ihre eigene Nachverfolgung und Verwaltung durch AWS WAF. Wenn Sie eine ratenbasierte Regel innerhalb einer Regelgruppe definieren und diese Regelgruppe dann an mehreren Stellen verwenden, erstellt jede Verwendung eine separate Instanz der ratenbasierten Regel, die ihre eigene Nachverfolgung und Verwaltung erhält. AWS WAF

Keine Verschachtelung – Sie können diesen Anweisungstyp nicht in andere Anweisungen einfügen. Sie können sie direkt in eine Web-ACL oder Regelgruppe aufnehmen.

Scope-Down Statement — Dieser Regeltyp kann eine Scope-down-Aussage enthalten, um den Umfang der Anfragen, die die Regel verfolgt, einzugrenzen und die Rate zu begrenzen. Die Scope-down-Aussage kann optional oder erforderlich sein, abhängig von Ihren anderen Regelkonfigurationseinstellungen. Die Einzelheiten werden in diesem Abschnitt behandelt.

Allgemeine Informationen zu Scopedown-Aussagen finden Sie unter [Eingrenzungsanweisungen](#)

WCUs — 2, als Basiskosten. Fügen Sie für jeden benutzerdefinierten Aggregationsschlüssel, den Sie angeben, 30 WCUs hinzu. Wenn Sie in der Regel eine Scopedown-Anweisung verwenden, berechnen Sie die entsprechenden WCUs und fügen Sie sie hinzu.

Wo finde ich diese Regelaussage

- Rule Builder in der Web-ACL auf der Konsole – Wählen Sie unter Rule (Regel) für Type (Typ) die Option Rate-based rule (Ratenbasierte Regel) aus.
- API — [RateBasedStatement](#)

Themen

- [Ratenbasierte Regeleinstellungen auf hoher Ebene](#)
- [Vorbehalte bei ratenbasierten Regeln](#)
- [Aggregationsoptionen und Schlüssel](#)
- [Aggregationsinstanzen und -zählungen](#)
- [Verhalten zur Begrenzung der Anforderungsrate](#)
- [Beispiele für ratenbasierte Regeln](#)
- [Auflisten von IP-Adressen, deren Rate durch ratenbasierte Regeln begrenzt wird](#)

Ratenbasierte Regeleinstellungen auf hoher Ebene

Eine ratenbasierte Regelanweisung verwendet die folgenden allgemeinen Einstellungen:

- Bewertungsfenster — Der Zeitraum in Sekunden, der in der Anzahl der Anfragen AWS WAF berücksichtigt werden soll, wenn man von der aktuellen Uhrzeit aus betrachtet. Beispiel: Bei einer Einstellung von 120 werden bei der AWS WAF Überprüfung der Rate die Anfragen für die 2 Minuten gezählt, die unmittelbar vor der aktuellen Uhrzeit liegen. Gültige Einstellungen sind 60 (1 Minute), 120 (2 Minuten), 300 (5 Minuten) und 600 (10 Minuten), und 300 (5 Minuten) ist die Standardeinstellung.

Diese Einstellung bestimmt nicht, wie oft die Rate AWS WAF überprüft wird, sondern wie weit sie bei jeder Überprüfung zurückblickt. AWS WAF überprüft die Rate regelmäßig, wobei der Zeitpunkt unabhängig von der Einstellung des Bewertungsfensters ist.

- Ratenlimit — Die maximale Anzahl von Anfragen, die Ihren Kriterien entsprechen und nur innerhalb des angegebenen Bewertungsfensters erfasst werden AWS WAF sollen. Die niedrigste zulässige

Grenzwerteinstellung ist 100. Wenn dieser Grenzwert überschritten wird, AWS WAF wendet die Einstellung für die Regelaktion auf weitere Anfragen an, die Ihren Kriterien entsprechen.

AWS WAF wendet eine Ratenbegrenzung in der Nähe des von Ihnen festgelegten Limits an, garantiert jedoch nicht, dass das Limit exakt übereinstimmt. Weitere Informationen finden Sie unter [Vorbehalte bei ratenbasierten Regeln](#).

- Aggregation von Anfragen — Die im Internet zu verwendenden Aggregationskriterien, die von der ratenbasierten Regel berücksichtigt werden, und die Ratenbegrenzungen. Das von Ihnen festgelegte Ratenlimit gilt für jede Aggregationsinstanz. Details dazu finden Sie unter [Aggregationsoptionen und Schlüssel](#) und [Aggregationsinstanzen und -zählungen](#).
- Aktion — Die Aktion, die bei Anfragen ergriffen werden soll, die von der Regelrate begrenzt werden. Sie können jede beliebige Regelaktion verwenden, außer Allow Dies wird wie üblich auf Regelebene festgelegt, weist jedoch einige Einschränkungen und Verhaltensweisen auf, die für ratenbasierte Regeln spezifisch sind. Allgemeine Informationen zu Regelaktionen finden Sie unter [Regelaktion](#). Spezifische Informationen zur Ratenbegrenzung finden Sie [Verhalten zur Begrenzung der Anforderungsrate](#) in diesem Abschnitt.
- Prüfungsumfang und Gebührenbegrenzung — Sie können den Umfang der Anfragen, die in der tarifbasierten Abrechnung erfasst werden, und die Preisbegrenzungen einschränken, indem Sie eine Erklärung zum Umfang hinzufügen. Wenn Sie eine Erklärung zum Umfang angeben, aggregiert, zählt und begrenzt die Regel nur Anfragen, die mit dem Umfang übereinstimmen. Wenn Sie die Anforderungsaggregationsoption Alle zählen wählen, ist die Scopedown-Anweisung erforderlich. Weitere Informationen zu Eingrenzungsanweisungen finden Sie unter [Eingrenzungsanweisungen](#).
- (Optional) Konfiguration für weitergeleitete IP-Adressen — Diese Konfiguration wird nur verwendet, wenn Sie die IP-Adresse im Header Ihrer Anforderungsaggregation angeben, entweder allein oder als Teil der Einstellungen für benutzerdefinierte Schlüssel. AWS WAF ruft die erste IP-Adresse im angegebenen Header ab und verwendet diese als Aggregationswert. Ein üblicher Header für diesen Zweck ist `X-Forwarded-For`, aber Sie können einen beliebigen Header angeben. Weitere Informationen finden Sie unter [Weitergeleitete IP-Adresse](#).

Vorbehalte bei ratenbasierten Regeln

AWS WAF Die Ratenbegrenzung dient dazu, hohe Anforderungsraten zu kontrollieren und die Verfügbarkeit Ihrer Anwendung so effizient und effektiv wie möglich zu schützen. Es ist nicht für eine präzise Begrenzung der Anforderungsrate vorgesehen.

- AWS WAF schätzt die aktuelle Anforderungsrate mithilfe eines Algorithmus, der neueren Anfragen mehr Bedeutung beimisst. Aus diesem Grund AWS WAF wird eine Ratenbegrenzung in der Nähe des von Ihnen festgelegten Limits angewendet, es wird jedoch nicht garantiert, dass das Limit exakt eingehalten wird.
- Jedes Mal, wenn die Rate der Anfragen AWS WAF geschätzt wird, AWS WAF wird die Anzahl der Anfragen berücksichtigt, die während des konfigurierten Testfensters eingegangen sind. Aufgrund dieser und anderer Faktoren, wie etwa Verzögerungen bei der Übertragung, ist es möglich, dass Anfragen mehrere Minuten lang mit einer zu hohen Rate eingehen, bevor sie AWS WAF erkannt und durch die Rate begrenzt werden. In ähnlicher Weise kann die Anforderungsrate für einen bestimmten Zeitraum unter dem Grenzwert liegen, bevor der Rückgang AWS WAF erkannt und die Maßnahme zur Ratenbegrenzung eingestellt wird. In der Regel liegt diese Verzögerung unter 30 Sekunden.
- Wenn Sie eine der Einstellungen für die Ratenbegrenzung in einer Regel ändern, die gerade verwendet wird, werden die Werte für die Ratenbegrenzung der Regel durch die Änderung zurückgesetzt. Dadurch können die Aktivitäten zur Ratenbegrenzung der Regel für bis zu einer Minute unterbrochen werden. Bei den Einstellungen für die Ratenbegrenzung handelt es sich um das Bewertungsfenster, das Ratenlimit, die Einstellungen für die Anforderungsaggregation, die Konfiguration der weitergeleiteten IP und den Inspektionsumfang.

Aggregationsoptionen und Schlüssel

Standardmäßig aggregiert und begrenzt eine ratenbasierte Regel Anfragen auf der Grundlage der Anfrage-IP-Adresse. Sie können die Regel so konfigurieren, dass sie verschiedene andere Aggregationsschlüssel und Tastenkombinationen verwendet. Sie können beispielsweise auf der Grundlage einer weitergeleiteten IP-Adresse, der HTTP-Methode oder eines Abfragearguments aggregieren. Sie können auch Aggregationsschlüsselkombinationen wie IP-Adresse und HTTP-Methode oder die Werte von zwei verschiedenen Cookies angeben.

Note

Alle Anforderungskomponenten, die Sie im Aggregationsschlüssel angeben, müssen in einer Webanforderung vorhanden sein, damit die Anforderung ausgewertet oder die Rate durch die Regel begrenzt wird.

Sie können Ihre ratenbasierte Regel mit den folgenden Aggregationsoptionen konfigurieren.

- Quell-IP-Adresse — Aggregieren Sie, indem Sie nur die IP-Adresse verwenden, aus der die Webanfrage stammt.

Die Quell-IP-Adresse enthält möglicherweise nicht die Adresse des ursprünglichen Clients. Wenn eine Webanfrage einen oder mehrere Proxys oder Load Balancer durchläuft, enthält diese die Adresse des letzten Proxys.

- IP-Adresse im Header — Aggregiert, wobei nur eine Clientadresse in einem HTTP-Header verwendet wird. Dies wird auch als weitergeleitete IP-Adresse bezeichnet.

Mit dieser Konfiguration geben Sie auch ein Fallback-Verhalten an, das auf eine Webanfrage mit einer falsch formatierten IP-Adresse im Header angewendet wird. Das Fallback-Verhalten legt das Übereinstimmungsergebnis für die Anforderung fest, auf Übereinstimmung oder keine Übereinstimmung. Wenn keine Übereinstimmung vorliegt, zählt die ratenbasierte Regel die Anfrage nicht und begrenzt sie auch nicht auf die Rate. Bei Übereinstimmung gruppiert die ratenbasierte Regel die Anfrage zusammen mit anderen Anfragen, deren IP-Adresse im angegebenen Header falsch formatiert ist.

Gehen Sie bei dieser Option vorsichtig vor, da Header von Proxys inkonsistent verarbeitet werden können und sie auch geändert werden können, um die Überprüfung zu umgehen. Weitere Informationen und bewährte Methoden finden Sie unter [Weitergeleitete IP-Adresse](#)

- Alle zählen — Zählt und begrenzt die Rate aller Anfragen, die dem Geltungsbereich der Regel entsprechen. Für diese Option ist eine Scope-down-Aussage erforderlich. Diese Option wird in der Regel verwendet, um die Rate einer bestimmten Gruppe von Anfragen zu begrenzen, z. B. für alle Anfragen mit einer bestimmten Bezeichnung oder für alle Anfragen aus einem bestimmten geografischen Gebiet.
- Benutzerdefinierte Schlüssel — Aggregieren Sie mithilfe eines oder mehrerer benutzerdefinierter Aggregationsschlüssel. Um eine der IP-Adressoptionen mit anderen Aggregationsschlüsseln zu kombinieren, definieren Sie sie hier unter benutzerdefinierte Schlüssel.

Benutzerdefinierte Aggregationsschlüssel sind eine Teilmenge der unter beschriebenen Optionen für Webanforderungskomponenten. [Anforderungskomponentenoptionen](#)

Die wichtigsten Optionen sind die folgenden. Sofern nicht anders angegeben, können Sie eine Option mehrfach verwenden, z. B. zwei Header oder drei Label-Namespaces.

- Label-Namespace — Verwenden Sie einen Label-Namespace als Aggregationsschlüssel. Jeder eindeutige vollqualifizierte Labelname, der den angegebenen Label-Namespace hat, trägt zur

Aggregationsinstanz bei. Wenn Sie nur einen Label-Namespace als Ihren benutzerdefinierten Schlüssel verwenden, definiert jeder Labelname eine Aggregationsinstanz vollständig.

Die ratenbasierte Regel verwendet nur Labels, die der Anforderung durch Regeln hinzugefügt wurden, die zuvor in der Web-ACL ausgewertet wurden.

Hinweise zu Label-Namespace und Namen finden Sie unter [Bezeichnungssyntax- und Benennungsanforderungen](#)

- Header — Verwenden Sie einen benannten Header als Aggregationsschlüssel. Jeder eindeutige Wert im Header trägt zur Aggregationsinstanz bei.

Der Header benötigt eine optionale Texttransformation. Siehe [Texttransformationen](#).

- Cookie — Verwenden Sie ein benanntes Cookie als Aggregationsschlüssel. Jeder eindeutige Wert im Cookie trägt zur Aggregationsinstanz bei.

Das Cookie benötigt eine optionale Texttransformation. Siehe [Texttransformationen](#).

- Abfrageargument — Verwenden Sie ein einzelnes Abfrageargument in der Anfrage als Aggregatschlüssel. Jeder eindeutige Wert für das benannte Abfrageargument trägt zur Aggregationsinstanz bei.

Für das Abfrageargument ist eine optionale Texttransformation erforderlich. Siehe [Texttransformationen](#).

- Abfragezeichenfolge — Verwenden Sie die gesamte Abfragezeichenfolge in der Anfrage als Aggregatschlüssel. Jede einzelne Abfragezeichenfolge trägt zur Aggregationsinstanz bei. Sie können diesen Schlüsseltyp einmal verwenden.

Für die Abfragezeichenfolge ist eine optionale Texttransformation erforderlich. Siehe [Texttransformationen](#).

- URI-Pfad — Verwenden Sie den URI-Pfad in der Anfrage als Aggregatschlüssel. Jeder eindeutige URI-Pfad trägt zur Aggregationsinstanz bei. Sie können diesen Schlüsseltyp einmal verwenden.

Für den URI-Pfad ist eine optionale Texttransformation erforderlich. Siehe [Texttransformationen](#).

- HTTP-Methode — Verwenden Sie die HTTP-Methode der Anfrage als Aggregatschlüssel. Jede einzelne HTTP-Methode trägt zur Aggregationsinstanz bei. Sie können diesen Schlüsseltyp einmal verwenden.

- IP-Adresse — Aggregiert, indem die IP-Adresse aus dem Ursprung der Webanfrage in Kombination mit anderen Schlüsseln verwendet wird.

Dies enthält möglicherweise nicht die Adresse des ursprünglichen Clients. Wenn eine Webanfrage einen oder mehrere Proxys oder Load Balancer durchläuft, enthält diese die Adresse des letzten Proxys.

- IP-Adresse im Header — Aggregiert, indem die Client-Adresse in einem HTTP-Header in Kombination mit anderen Schlüsseln verwendet wird. Dies wird auch als weitergeleitete IP-Adresse bezeichnet.

Gehen Sie bei dieser Option vorsichtig vor, da Header von Proxys inkonsistent behandelt werden können und sie so geändert werden können, dass sie die Überprüfung umgehen. Weitere Informationen und bewährte Methoden finden Sie unter [Weitergeleitete IP-Adresse](#)

Aggregationsinstanzen und -zählungen

Wenn eine ratenbasierte Regel Webanfragen anhand Ihrer Aggregationskriterien auswertet, definiert jeder eindeutige Satz von Werten, den die Regel für die angegebenen Aggregationsschlüssel findet, eine eindeutige Aggregationsinstanz.

- Mehrere Schlüssel — Wenn Sie mehrere benutzerdefinierte Schlüssel definiert haben, trägt der Wert für jeden Schlüssel zur Definition der Aggregationsinstanz bei. Jede eindeutige Kombination von Werten definiert eine Aggregationsinstanz.
- Einzelner Schlüssel — Wenn Sie einen einzelnen Schlüssel ausgewählt haben, entweder in den benutzerdefinierten Schlüsseln oder indem Sie eine der Singleton-IP-Adressen ausgewählt haben, definiert jeder eindeutige Wert für den Schlüssel eine Aggregationsinstanz.
- Alle zählen — keine Schlüssel — Wenn Sie die Aggregationsoption Alle zählen ausgewählt haben, gehören alle Anfragen, die die Regel auswertet, zu einer einzigen Aggregationsinstanz für die Regel. Für diese Auswahl ist eine Scopedown-Aussage erforderlich.

Eine ratenbasierte Regel zählt Webanfragen für jede Aggregationsinstanz, die sie identifiziert, separat.

Nehmen wir beispielsweise an, eine ratenbasierte Regel wertet Webanfragen mit den folgenden IP-Adressen und HTTP-Methodenwerten aus:

- IP-Adresse 10.1.1.1, HTTP-Methode POST

- IP-Adresse 10.1.1.1, HTTP-Methode GET
- IP-Adresse 127.0.0.0, HTTP-Methode POST
- IP-Adresse 10.1.1.1, HTTP-Methode GET

Die Regel erstellt verschiedene Aggregationsinstanzen gemäß Ihren Aggregationskriterien.

- Wenn es sich bei den Aggregationskriterien nur um die IP-Adresse handelt, handelt es sich bei jeder einzelnen IP-Adresse um eine Aggregationsinstanz, und die Anfragen werden für jede Adresse AWS WAF separat gezählt. In unserem Beispiel wären die Aggregationsinstanzen und die Anzahl der Anfragen wie folgt:
 - IP-Adresse 10.1.1.1: Anzahl 3
 - IP-Adresse 127.0.0.0: Anzahl 1
- Wenn das Aggregationskriterium eine HTTP-Methode ist, ist jede einzelne HTTP-Methode eine Aggregationsinstanz. In unserem Beispiel wären die Aggregationsinstanzen und die Anzahl der Anfragen wie folgt:
 - HTTP-Methode POST: Anzahl 2
 - HTTP-Methode GET: Anzahl 2
- Wenn es sich bei den Aggregationskriterien um IP-Adresse und HTTP-Methode handelt, würden jede IP-Adresse und jede HTTP-Methode zur kombinierten Aggregationsinstanz beitragen. In unserem Beispiel wären die Aggregationsinstanzen und die Anzahl der Anfragen wie folgt:
 - IP-Adresse 10.1.1.1, HTTP-Methode POST: Anzahl 1
 - IP-Adresse 10.1.1.1, HTTP-Methode GET: Anzahl 2
 - IP-Adresse 127.0.0.0, HTTP-Methode POST: Anzahl 1

Verhalten zur Begrenzung der Anforderungsrate

Die Kriterien, AWS WAF anhand derer Limitanforderungen für eine ratenbasierte Regel bewertet werden, sind dieselben Kriterien, die für die Zusammenfassung von Anfragen für die Regel AWS WAF verwendet werden. Wenn Sie eine Scopedown-Aussage für die Regel definieren, werden AWS WAF nur Anfragen aggregiert, gezählt und begrenzt die Rate, die der Scope-Down-Anweisung entsprechen.

Die Übereinstimmungskriterien, die dazu führen, dass eine ratenbasierte Regel ihre Regelaktionseinstellungen auf eine bestimmte Webanforderung anwendet, lauten wie folgt:

- Die Webanforderung entspricht der Scope-Down-Anweisung der Regel, sofern eine definiert ist.
- Die Webanforderung gehört zu einer Aggregationsinstanz, deren Anzahl der Anfragen derzeit den Grenzwert der Regel überschreitet.

Wie AWS WAF wendet die Regelaktion an

Wenn eine ratenbasierte Regel eine Ratenbegrenzung auf eine Anfrage anwendet, wendet sie die Regelaktion an. Wenn Sie in Ihrer Aktionsspezifikation eine benutzerdefinierte Handhabung oder Kennzeichnung definiert haben, wendet die Regel diese an. Diese Bearbeitung von Anfragen entspricht der Art und Weise, wie eine Vergleichsregel ihre Aktionseinstellungen auf passende Webanfragen anwendet. Eine ratenbasierte Regel wendet nur Bezeichnungen an oder führt andere Aktionen auf Anfragen aus, für die sie aktiv die Rate begrenzt.

Sie können jede Regelaktion verwenden, außer... Allow Allgemeine Informationen zu Regelaktionen finden Sie unter [Regelaktion](#).

In der folgenden Liste wird beschrieben, wie die Ratenbegrenzung für die einzelnen Aktionen funktioniert.

- **Block**— AWS WAF blockiert die Anfrage und wendet jedes benutzerdefinierte Blockierungsverhalten an, das Sie definiert haben.
- **Count**— AWS WAF zählt die Anfrage, wendet alle benutzerdefinierten Header oder Labels an, die Sie definiert haben, und setzt die Web-ACL-Auswertung der Anfrage fort.

Durch diese Aktion wird die Anzahl der Anfragen nicht begrenzt. Es werden nur die Anfragen gezählt, die das Limit überschreiten.

- **CAPTCHA oder Challenge** — AWS WAF behandelt die Anfrage entweder wie eine Block oder wie eine Count, abhängig vom Status des Tokens der Anfrage.

Diese Aktion begrenzt nicht die Anzahl der Anfragen, die gültige Token haben. Sie begrenzt die Anzahl der Anfragen, die das Limit überschreiten und denen auch gültige Token fehlen.

- Wenn die Anfrage kein gültiges, noch nicht abgelaufenes Token hat, blockiert die Aktion die Anfrage und sendet das CAPTCHA-Puzzle oder die Browser-Challenge zurück an den Client.

Wenn der Endbenutzer oder der Client-Browser erfolgreich reagiert, erhält der Client ein gültiges Token und sendet die ursprüngliche Anfrage automatisch erneut. Wenn die Ratenbegrenzung für die Aggregationsinstanz weiterhin gilt, wird auf diese neue Anfrage mit dem gültigen, nicht abgelaufenen Token die Aktion angewendet, wie im nächsten Aufzählungspunkt beschrieben.

- Wenn die Anfrage über ein gültiges, noch nicht abgelaufenes Token verfügt, überprüft die Challenge Aktion CAPTCHA oder das Token und führt keine Aktion für die Anfrage aus, ähnlich wie bei der Aktion. Count Die ratenbasierte Regel gibt die Auswertung der Anfrage an die Web-ACL zurück, ohne eine abschließende Aktion zu ergreifen, und die Web-ACL setzt ihre Auswertung der Anfrage fort.

Weitere Informationen finden Sie unter [CAPTCHAund Challenge in AWS WAF](#).

Wenn Sie nur die IP-Adresse oder die weitergeleitete IP-Adresse einschränken

Wenn Sie die Regel so konfigurieren, dass nur die IP-Adresse für weitergeleitete IP-Adressen begrenzt wird, kann die Regelinstanz die Ratenbegrenzung auf bis zu 10.000 IP-Adressen beschränken. Wenn eine Regelinstanz mehr als 10.000 IP-Adressen für die Ratenbegrenzung identifiziert, beschränkt sie nur die 10.000 höchsten Absender.

Mit dieser Konfiguration können Sie die Liste der IP-Adressen abrufen, für die eine ratenbasierte Regel derzeit eine Ratenbegrenzung vorsieht. Wenn Sie eine Scope-Down-Anweisung verwenden, sind nur die Anfragen in der IP-Liste ratenbegrenzt, die der Scope-Down-Anweisung entsprechen. Hinweise zum Abrufen der IP-Adressliste finden Sie unter [Auflisten von IP-Adressen, deren Rate durch ratenbasierte Regeln begrenzt wird](#)

Beispiele für ratenbasierte Regeln

In diesem Abschnitt werden Beispielkonfigurationen für eine Vielzahl gängiger Anwendungsfälle für ratenbasierte Regeln beschrieben.

Jedes Beispiel enthält eine Beschreibung des Anwendungsfalls und zeigt dann in JSON-Auflistungen die Lösung für die benutzerdefiniert konfigurierten Regeln an.

Note

Die in diesen Beispielen gezeigten JSON-Auflistungen wurden in der Konsole erstellt, indem die Regel konfiguriert und dann mit dem Rule JSON editor (JSON-Regel-Editor) bearbeitet wurde.

Themen

- [Ratenbegrenzung der Anfragen auf eine Anmeldeseite](#)

- [Ratenbegrenzung der Anfragen an eine Anmeldeseite von einer beliebigen IP-Adresse oder einem beliebigen User-Agent-Paar](#)
- [Ratenbegrenzung der Anfragen, denen ein bestimmter Header fehlt](#)
- [Ratenbegrenzung der Anfragen mit bestimmten Labels](#)
- [Ratenbegrenzung der Anfragen für Labels, die einen bestimmten Label-Namespace haben](#)

Ratenbegrenzung der Anfragen auf eine Anmeldeseite

Um die Anzahl der Anfragen an die Anmeldeseite auf Ihrer Website zu begrenzen, ohne die Zugriffe auf den Rest Ihrer Website zu beeinträchtigen, könnten Sie eine ratenbasierte Regel mit einer Scopedown-Aussage erstellen, die Anfragen an Ihre Anmeldeseite abgleicht, und bei der die Anforderungsaggregation auf Alle zählen gesetzt ist.

Die ratenbasierte Regel zählt alle Anfragen für die Anmeldeseite in einer einzigen Aggregationsinstanz und wendet die Regelaktion an, wenn die Anfragen das Limit überschreiten.

Die folgende JSON-Liste zeigt ein Beispiel für diese Regelkonfiguration. Die Aggregationsoption Count All ist im JSON als Einstellung CONSTANT aufgeführt. Dieses Beispiel entspricht Anmeldeseiten, die mit /login beginnen.

```
{
  "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
      }
    ]
  }
}
```

Ratenbegrenzung der Anfragen an eine Anmeldeseite von einer beliebigen IP-Adresse oder einem beliebigen User-Agent-Paar

Um die Anzahl der Anfragen an die Anmeldeseite auf Ihrer Website für IP-Adressen und Benutzeragentenpaare, die Ihr Limit überschreiten, zu begrenzen, setzen Sie die Anforderungsaggregation auf Benutzerdefinierte Schlüssel und geben Sie die Aggregationskriterien an.

Die folgende JSON-Liste zeigt ein Beispiel für diese Regelkonfiguration. In diesem Beispiel haben wir das Limit auf 100 Anfragen in einem beliebigen Zeitraum von fünf Minuten pro IP-Adresse und Benutzeragent-Paar festgelegt.

```
{
  "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
      }
    ]
  }
}
}
```

Ratenbegrenzung der Anfragen, denen ein bestimmter Header fehlt

Um die Anzahl der Anfragen zu begrenzen, denen ein bestimmter Header fehlt, können Sie die Aggregationsoption `Count all` mit einer `Scope-Down-Anweisung` verwenden. Konfigurieren Sie die `Scope-Down-Anweisung` mit einer logischen Anweisung, die eine `NOT` Anweisung enthält, die nur dann `true` zurückgibt, wenn der Header existiert und einen Wert hat.

Die folgende JSON-Liste zeigt ein Beispiel für diese Regelkonfiguration.

```
{
  "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
                }
              ]
            }
          }
        }
      }
    }
  }
}
```

Ratenbegrenzung der Anfragen mit bestimmten Labels

Sie können die Ratenbegrenzung mit jeder Regel oder Regelgruppe kombinieren, die Anforderungen mit Labels versehen, um die Anzahl der Anfragen verschiedener Kategorien zu begrenzen. Dazu konfigurieren Sie Ihre Web-ACL wie folgt:

- Fügen Sie die Regeln oder Regelgruppen hinzu, die Labels hinzufügen, und konfigurieren Sie sie so, dass sie die Anfragen, deren Rate begrenzt werden soll, nicht blockieren oder zulassen. Wenn Sie verwaltete Regelgruppen verwenden, müssen Sie möglicherweise einige Regelgruppenregelaktionen überschreiben, Count um dieses Verhalten zu erreichen.
- Fügen Sie Ihrer Web-ACL eine ratenbasierte Regel mit einer Prioritätsnummer hinzu, die über den Labeling-Regeln und Regelgruppen liegt. AWS WAF wertet Regeln in numerischer Reihenfolge aus, beginnend mit der niedrigsten, sodass Ihre ratenbasierte Regel nach den Labeling-Regeln ausgeführt wird. Konfigurieren Sie Ihre Ratenbegrenzung für die Labels mithilfe einer Kombination aus dem Label-Abgleich in der Scopedown-Anweisung der Regel und der Label-Aggregation.

Im folgenden Beispiel wird die Regelgruppe AWS Managed Rules der Amazon IP-Reputationsliste verwendet. Die Regelgruppenregel `AWSManagedIPDDoSList` erkennt und kennzeichnet Anfragen, deren IP-Adressen bekanntermaßen aktiv an DDoS-Aktivitäten beteiligt sind. Die Aktion der Regel ist Count in der Regelgruppendefinition so konfiguriert. Weitere Informationen zur Regelgruppe finden Sie unter [the section called “Amazon IP Reputation List”](#).

In der folgenden Web-ACL-JSON-Liste wird die IP-Reputationsregelgruppe verwendet, gefolgt von einer Regel, die auf der Rate des Labelabgleichs basiert. Die ratenbasierte Regel verwendet eine Scopedown-Anweisung, um nach Anfragen zu filtern, die durch die Regelgruppenregel gekennzeichnet wurden. Die ratenbasierte Regelanweisung aggregiert die gefilterten Anfragen anhand ihrer IP-Adressen und begrenzt die Rate.

```
{
  "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": "aws:waf: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": "aws:waf:000000000000:webacl:test-web-acl:"  
}
```

Ratenbegrenzung der Anfragen für Labels, die einen bestimmten Label-Namespace haben

Die allgemeinen Regeln in der verwalteten Regelgruppe Bot Control fügen Labels für Bots verschiedener Kategorien hinzu, blockieren aber nur Anfragen von nicht verifizierten Bots. Informationen zu diesen Regeln finden Sie unter [Liste der Bot-Control-Regeln](#).

Wenn Sie die verwaltete Regelgruppe Bot Control verwenden, können Sie eine Ratenbegrenzung für Anfragen von einzelnen verifizierten Bots hinzufügen. Dazu fügst du eine ratenbasierte Regel hinzu, die nach der Bot Control-Regelgruppe ausgeführt wird und Anfragen nach ihren Bot-Namensbezeichnungen zusammenfasst. Sie geben den Aggregationsschlüssel des Label-Namespace an und setzen den Namespace-Schlüssel auf. `aws:waf:managed:aws:bot-control:bot:name`: Jedes eindeutige Label mit dem angegebenen Namespace definiert eine Aggregationsinstanz. Zum Beispiel definieren die Labels `aws:waf:managed:aws:bot-control:bot:name:axios` und `aws:waf:managed:aws:bot-control:bot:name:curl` jedes Label eine Aggregationsinstanz.

Die folgende Web-ACL-JSON-Liste zeigt diese Konfiguration. Die Regel in diesem Beispiel begrenzt Anfragen für eine einzelne Bot-Aggregationsinstanz auf 1.000 innerhalb von zwei Minuten.

```
{  
  "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": "aws-waf:0000000000:webacl:test-web-acl:"  
}
```

Auflisten von IP-Adressen, deren Rate durch ratenbasierte Regeln begrenzt wird

Wenn Ihre ratenbasierte Regel nur nach IP-Adressen oder weitergeleiteten IP-Adressen aggregiert, können Sie die Liste der IP-Adressen abrufen, für die die Regel derzeit eine Ratenbegrenzung vorsieht. AWS WAF speichert diese IP-Adressen in der Liste der verwalteten Schlüssel der Regel.

Note

Diese Option ist nur verfügbar, wenn Sie nur die IP-Adresse oder nur eine IP-Adresse in einem Header aggregieren. Wenn Sie die Anforderungsaggregation für benutzerdefinierte Schlüssel verwenden, können Sie keine Liste mit IP-Adressen mit begrenzter Geschwindigkeit abrufen, selbst wenn Sie eine der IP-Adressspezifikationen in Ihren benutzerdefinierten Schlüsseln verwenden.

Eine ratenbasierte Regel wendet ihre Regelaktion auf Anfragen aus der Liste der verwalteten Schlüssel der Regel an, die der Scopedown-Anweisung der Regel entsprechen. Wenn eine Regel keine Scope-down-Anweisung enthält, wendet sie die Aktion auf alle Anfragen von den IP-Adressen an, die in der Liste aufgeführt sind. Die Regelaktion ist Block standardmäßig, es kann sich aber auch um jede gültige Regelaktion handeln, mit Ausnahme von Allow. Die maximale Anzahl von IP-Adressen, für die AWS WAF eine Ratenbegrenzung mit einer einzigen ratenbasierten Regelinstanz möglich ist, beträgt 10.000. Wenn mehr als 10.000 Adressen das Ratenlimit überschreiten, werden die Adressen mit den höchsten Raten AWS WAF begrenzt.

Sie können über die CLI, die API oder eines der SDKs auf die Liste der verwalteten Schlüssel einer ratenbasierten Regel zugreifen. In diesem Thema wird der Zugriff über CLI und APIs behandelt. Die Konsole bietet derzeit keinen Zugriff auf die Liste.

Für die AWS WAF API lautet der Befehl [GetRateBasedStatementManagedKeys](#).

Für die AWS WAF CLI lautet der Befehl [get-rate-based-statement-managed-keys](#).

Im Folgenden wird die Syntax zum Abrufen der Liste der ratenbegrenzten IP-Adressen für eine ratenbasierte Regel gezeigt, die in einer Web-ACL auf einer Amazon-Distribution verwendet wird.
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
```

Im Folgenden wird die Syntax für eine regionale Anwendung, eine Amazon API Gateway Gateway-REST-API, einen Application Load Balancer, eine AWS AppSync GraphQL-API, einen Amazon Cognito Cognito-Benutzerpool, einen AWS App Runner Service oder eine AWS Verified Access-Instance gezeigt.

```
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 überwacht Webanfragen und verwaltet Schlüssel unabhängig für jede eindeutige Kombination aus Web-ACL, optionaler Regelgruppe und ratenbasierter Regel. Wenn Sie beispielsweise eine ratenbasierte Regel in einer Regelgruppe definieren und die Regelgruppe dann in einer Web-ACL verwenden, überwacht AWS WAF Webanforderungen und verwaltet Schlüssel für diese Web-ACL, die Referenzanweisung der Regelgruppe und die Instance der ratenbasierten Regel. Wenn Sie dieselbe Regelgruppe in einer zweiten Web-ACL verwenden, AWS WAF überwacht Webanfragen und verwaltet Schlüssel für diese zweite Verwendung völlig unabhängig von Ihrer ersten.

Für eine ratenbasierte Regel, die Sie innerhalb einer Regelgruppe definiert haben, müssen Sie in Ihrer Anfrage zusätzlich zum Web-ACL-Namen und dem Namen der ratenbasierten Regel innerhalb der Regelgruppe den Namen der Referenzanweisung für die Regelgruppe angeben. Im Folgenden wird die Syntax für eine regionale Anwendung gezeigt, bei der die ratenbasierte Regel innerhalb einer Regelgruppe definiert ist und die Regelgruppe in einer Web-ACL verwendet wird.

```
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
```

Regelgruppenregelanweisungen

Regelgruppen-Regelanweisungen sind nicht verschachtelbar.

In diesem Abschnitt werden die Regelgruppenregelanweisungen beschrieben, die Sie in Ihrer Web-ACL verwenden können. Die Kapazitätseinheiten (WCUs) für Web-ACLs für Regelgruppen werden vom Eigentümer der Regelgruppe zum Zeitpunkt der Erstellung festgelegt. Informationen zu den WCUs finden Sie unter [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#).

Regelgruppenanweisung	Beschreibung	WCUs
Verwaltete Regelgruppe	<p>Führt die Regeln aus, die in der angegebenen verwalteten Regelgruppe definiert sind.</p> <p>Sie können den Umfang der Anfragen, die die Regelgruppe auswertet, einschränken, indem Sie eine Scopedown-Anweisung hinzufügen.</p> <p>Sie können eine verwaltete Regelgruppenanweisung nicht innerhalb eines anderen Anweisungstyps verschachteln.</p>	Definiert durch die Regelgruppe sowie alle zusätzlichen WCUs für eine Scopedown-Anweisung.
Regelgruppe	<p>Führt die Regeln aus, die in einer Regelgruppe definiert sind, die Sie verwalten.</p> <p>Sie können einer Regelgruppen-Referenzaussage für Ihre eigene Regelgruppe keine Scopedown-Anweisung hinzufügen.</p>	Das WCU-Limit legen Sie beim Anlegen für die Regelgruppe fest.

Regelgruppenanweisung	Beschreibung	WCUs
	Sie können eine Regelgruppenanweisung nicht innerhalb einer anderen Anweisungstyps verschachteln	

Verwaltete Regelgruppenanweisung

Die Regelanweisung für verwaltete Regelgruppen fügt einen Verweis in Ihrer Web-ACL-Regelliste zu einer verwalteten Regelgruppe hinzu. Sie sehen diese Option nicht in Ihren Regelanweisungen in der Konsole, aber wenn Sie mit dem JSON-Format Ihrer Web-ACL arbeiten, werden alle verwalteten Regelgruppen, die Sie hinzugefügt haben, unter den Web-ACL-Regeln als dieser Typ angezeigt.

Eine verwaltete Regelgruppe ist entweder eine Regelgruppe mit AWS verwalteten Regeln, von denen die meisten für AWS WAF Kunden kostenlos sind, oder eine AWS Marketplace verwaltete Regelgruppe. Sie abonnieren automatisch die kostenpflichtigen Regelgruppen für AWS verwaltete Regeln, wenn Sie sie zu Ihrer Web-ACL hinzufügen. Sie können AWS Marketplace verwaltete Regelgruppen über abonnieren AWS Marketplace. Weitere Informationen finden Sie unter [Verwaltete Regelgruppen](#).

Wenn Sie einer Web-ACL eine Regelgruppe hinzufügen, können Sie die Aktionen der Regeln in der Gruppe durch Count oder durch eine andere Regelaktion überschreiben. Weitere Informationen finden Sie unter [Aktionsüberschreibungen in Regelgruppen](#).

Sie können den Umfang der Anfragen einschränken, die anhand der Regelgruppe AWS WAF ausgewertet werden. Dazu fügen Sie eine Eingrenzungsanweisung innerhalb der Regelgruppenanweisung hinzu. Informationen zu Eingrenzungsanweisungen finden Sie unter [Eingrenzungsanweisungen](#). Das kann Ihnen helfen, zu verwalten, wie sich die Regelgruppe auf Ihren Datenverkehr auswirkt, und die mit dem Verkehrsvolumen verbundenen Kosten einzudämmen, wenn Sie die Regelgruppe verwenden. Informationen und Beispiele für die Verwendung von Scopedown-Anweisungen mit der verwalteten Regelgruppe von AWS WAF Bot Control finden Sie unter [AWS WAF Bot-Steuerung](#).

Keine Verschachtelung – Sie können diesen Anweisungstyp nicht in andere Anweisungen einfügen und ihn auch nicht in eine Regelgruppe aufnehmen. Sie können sie direkt in eine Web-ACL aufnehmen.

(Optional) Eingrenzungsanweisung – Dieser Regeltyp benötigt eine optionale Eingrenzungsanweisung, um einzuschränken, welche Anforderungen die Regelgruppe auswertet. Weitere Informationen finden Sie unter [Eingrenzungsanweisungen](#).

WCUs – wird beim Anlegen für die Regelgruppe festgelegt.

Wo finde ich diese Regelaussage

- Konsole – Wählen Sie während des Erstellungsprozesses einer Web-ACL auf der Seite Add rules and rule groups (Regeln und Regelgruppen hinzufügen) die Option Add managed rule groups (Verwaltete Regelgruppen hinzufügen) aus. Wählen Sie dann die Regelgruppe aus, die Sie verwenden möchten.
- API — [ManagedRuleGroupStatement](#)

Regelgruppenanweisung

Die Regelgruppenregelanweisung fügt einer von Ihnen verwalteten Regelgruppe einen Verweis auf Ihre Web-ACL-Regelliste hinzu. Sie sehen diese Option nicht in Ihren Regelanweisungen in der Konsole, aber wenn Sie mit dem JSON-Format Ihrer Web-ACL arbeiten, werden Ihr eigenen Regelgruppen, die Sie hinzugefügt haben, unter den Web-ACL-Regeln als dieser Typ angezeigt. Informationen zur Verwendung eigener Regelgruppen finden Sie unter [Verwaltung Ihrer eigenen Regelgruppen](#).

Wenn Sie einer Web-ACL eine Regelgruppe hinzufügen, können Sie die Aktionen der Regeln in der Gruppe durch Count oder durch eine andere Regelaktion überschreiben. Weitere Informationen finden Sie unter [Aktionsüberschreibungen in Regelgruppen](#).

Keine Verschachtelung – Sie können diesen Anweisungstyp nicht in andere Anweisungen einfügen und ihn auch nicht in eine Regelgruppe aufnehmen. Sie können sie direkt in eine Web-ACL aufnehmen.

WCUs – wird beim Anlegen für die Regelgruppe festgelegt.

Wo finde ich diese Regelaussage

- Konsole – Wählen Sie während des Erstellungsprozesses einer Web-ACL auf der Seite Add rules and rule groups (Regeln und Regelgruppen hinzufügen), Add my own rules and rule groups (Eigene Regeln und Regelgruppen hinzufügen) und Rule group (Regelgruppe) aus. Fügen Sie dann die Regelgruppe hinzu, die Sie verwenden möchten.

- API — [RuleGroupReferenceStatement](#)

Umgang mit übergroßen Webanforderungskomponenten in AWS WAF

AWS WAF unterstützt nicht die Überprüfung sehr großer Inhalte für den Hauptteil, die Header oder Cookies der Webanforderungskomponenten. Der zugrundeliegende Hostdienst hat Beschränkungen hinsichtlich der Anzahl und Größe der Daten, an die er zur AWS WAF Überprüfung weiterleitet. Beispielsweise sendet der Hostdienst nicht mehr als 200 Header an AWS WAF, sodass bei einer Webanfrage mit 205 Headern die letzten 5 Header nicht überprüft AWS WAF werden können.

Wenn AWS WAF eine Webanfrage an Ihre geschützte Ressource weitergeleitet werden kann, wird die gesamte Webanforderung gesendet, einschließlich aller Inhalte, die außerhalb der Anzahl und Größe liegen, die überprüft werden AWS WAF konnte.

Größenbeschränkungen bei der Inspektion von Komponenten

Die Größenbeschränkungen für die Inspektion von Komponenten lauten wie folgt:

- **Body** und **JSON Body** — Für Application Load Balancer und AWS AppSync AWS WAF können die ersten 8 KB des Hauptteils einer Anfrage untersuchen. Denn CloudFront API Gateway, Amazon Cognito, App Runner und Verified Access AWS WAF können standardmäßig die ersten 16 KB überprüfen, und Sie können das Limit in Ihrer Web-ACL-Konfiguration auf bis zu 64 KB erhöhen. Weitere Informationen finden Sie unter [Verwaltung der Größenbeschränkungen bei Körperinspektionen](#).
- **Headers** — AWS WAF kann höchstens die ersten 8 KB (8.192 Byte) der Anforderungsheader und höchstens die ersten 200 Header untersuchen. Der Inhalt kann AWS WAF bis zum ersten erreichten Limit überprüft werden.
- **Cookies** — AWS WAF kann höchstens die ersten 8 KB (8.192 Byte) der Anforderungs-Cookies und höchstens die ersten 200 Cookies untersuchen. Der Inhalt kann AWS WAF bis zum ersten erreichten Limit eingesehen werden.

Überdimensionierte Bearbeitungsoptionen für Ihre Regelaussagen

Wenn Sie eine Regelanweisung schreiben, die einen dieser Anforderungskomponententypen untersucht, geben Sie an, wie mit übergroßen Komponenten umgegangen werden soll. Die Behandlung von Übergrößen gibt an, AWS WAF was mit einer Webanforderung geschehen

soll, wenn die von der Regel untersuchte Anforderungskomponente die Größenbeschränkungen überschreitet.

Die Optionen für den Umgang mit übergroßen Komponenten lauten wie folgt:

- **Continue**— Untersuchen Sie die Anforderungskomponente normal gemäß den Regelprüfungskriterien. AWS WAF überprüft den Inhalt der Anforderungskomponente, der innerhalb der Größenbeschränkungen liegt.
- **Match**— Behandelt die Webanforderung so, als ob sie der Regelanweisung entspricht. AWS WAF wendet die Regelaktion auf die Anfrage an, ohne sie anhand der Prüfkriterien der Regel zu bewerten.
- **No match**— Behandelt die Webanforderung als nicht übereinstimmend mit der Regelaussage, ohne sie anhand der Prüfkriterien der Regel zu bewerten. AWS WAF setzt die Prüfung der Webanforderung fort und verwendet dabei die restlichen Regeln in der Web-ACL, wie dies bei jeder Regel der Fall wäre, die nicht übereinstimmend ist.

In der AWS WAF Konsole müssen Sie eine dieser Behandlungsoptionen auswählen. Außerhalb der Konsole ist die Standardoption `Continue`.

Wenn Sie die `Match` Option in einer Regel verwenden, deren Aktion auf `Block` gesetzt ist, blockiert die Regel eine Anfrage, deren überprüfte Komponente zu groß ist. Bei jeder anderen Konfiguration hängt die endgültige Bearbeitung der Anforderung von verschiedenen Faktoren ab, z. B. von der Konfiguration der anderen Regeln in Ihrer Web-ACL und der Standardaktionseinstellung der Web-ACL.

Umgang mit überdimensionalen Regelgruppen, deren Eigentümer Sie nicht sind

Beschränkungen für die Größe und Anzahl der Komponenten gelten für alle Regeln, die Sie in Ihrer Web-ACL verwenden. Dazu gehören alle Regeln, die Sie verwenden, aber nicht verwalten, in verwalteten Regelgruppen und in Regelgruppen, die von einem anderen Konto für Sie freigegeben wurden.

Wenn Sie eine Regelgruppe verwenden, die Sie nicht verwalten, verfügt die Regelgruppe möglicherweise über eine Regel, die eine eingeschränkte Anforderungskomponente überprüft, übergroße Inhalte jedoch nicht so behandelt, wie Sie sie benötigen. Informationen darüber, wie AWS verwaltete Regeln übergroße Komponenten verwalten, finden Sie unter [AWS Liste der Regelgruppen für verwaltete Regeln](#). Wenden Sie sich an Ihren Regelgruppenanbieter, um Informationen zu anderen Regelgruppen zu erhalten.

Richtlinien für die Verwaltung übergroßer Komponenten in Ihrer Web-ACL

Die Art und Weise, wie Sie übergroße Komponenten in Ihrer Web-ACL behandeln, hängt von einer Reihe von Faktoren ab, wie der erwarteten Größe des Inhalts Ihrer Anforderungskomponente, der standardmäßigen Behandlung von Anforderungen durch Ihre Web-ACL und der Art und Weise, wie andere Regeln in Ihrer Web-ACL Anforderungen abgleichen und verarbeiten.

Die allgemeinen Richtlinien für die Verwaltung übergroßer Webanforderungskomponenten lauten wie folgt:

- Wenn Sie Anforderungen mit übergroßen Komponenteninhalten zulassen müssen, fügen Sie nach Möglichkeit Regeln hinzu, um nur diese Anforderungen explizit zuzulassen. Priorisieren Sie diese Regeln so, dass sie vor anderen Regeln in der Web-ACL ausgeführt werden, die dieselben Komponententypen prüfen. Mit diesem Ansatz können Sie nicht den gesamten Inhalt der übergroßen Komponenten überprüfen, die Sie an Ihre geschützte Ressource weitergeben dürfen.
AWS WAF
- Für alle anderen Anforderungen können Sie verhindern, dass zusätzliche Bytes übergeben werden, indem Sie Anforderungen blockieren, die das Limit überschreiten:
 - Ihre Regeln und Regelgruppen — Konfigurieren Sie in Ihren Regeln zur Prüfung von Komponenten mit Größenbeschränkungen den Umgang mit überdimensionalen Komponenten so, dass Sie Anfragen blockieren, die das Limit überschreiten. Wenn Ihre Regel beispielsweise Anfragen mit bestimmten Header-Inhalten blockiert, legen Sie die Behandlung von Übergrößen so fest, dass sie auch Anfragen mit übergroßen Header-Inhalten entspricht. Wenn Ihre Web-ACL Anfragen standardmäßig blockiert und Ihre Regel bestimmte Header-Inhalte zulässt, konfigurieren Sie alternativ die Behandlung zu großer Größe Ihrer Regel so, dass sie bei Anfragen mit übergroßen Header-Inhalten nicht übereinstimmt.
 - Regelgruppen, die Sie nicht verwalten – Um zu verhindern, dass Regelgruppen, die Sie nicht verwalten, übergroße Anforderungskomponenten zulassen, können Sie eine separate Regel hinzufügen, die den Anforderungskomponententyp überprüft und Anforderungen blockiert, die Grenzwerte überschreiten. Priorisieren Sie die Regel in Ihrer Web-ACL, damit sie vor den Regelgruppen ausgeführt wird. Sie können beispielsweise Anforderungen mit übergroßen Textinhalten blockieren, bevor eine Ihrer Regeln für die Textüberprüfung in der Web-ACL ausgeführt wird. Im folgenden Verfahren wird beschrieben, wie dieser Regeltyp hinzugefügt wird.

So fügen Sie eine Regel hinzu, die übergroße Inhalte blockiert

1. Wenn Sie eine Web-ACL erstellen oder bearbeiten, wählen Sie in den Regeleinstellungen Add rules (Hinzufügen von Regeln), Add my own rules and rule groups (Eigene Regeln und Regelgruppen hinzufügen), Rule Builder (Regel erstellen) und dann Rule visual editor (Visueller Editor für Regel) aus. Anleitungen zum Erstellen oder Bearbeiten einer Web-ACL finden Sie unter [Arbeiten mit Web-ACLs](#)
2. Geben Sie einen Namen für die Regel ein und lassen Sie die Einstellung Type (Typ) auf Regular rule (Reguläre Regel) eingestellt.
3. Ändern Sie die folgenden Übereinstimmungseinstellungen:
 - a. Öffnen Sie unter Statement (Anweisung) das Drop-down-Menü für Inspect (Untersuchen) und wählen Sie die benötigte Webanforderungskomponente aus, also entweder Body (Text), Headers (Header) oder Cookies.
 - b. Wählen Sie für Match type (Übereinstimmungstyp) die Option Size greater than (Größe größer als) aus.
 - c. Geben Sie unter Größe eine Zahl ein, die mindestens der Mindestgröße für den Komponententyp entspricht. Geben Sie für Header und Cookies Folgendes ein 8192. Geben Sie in Application Load Balancer oder AWS AppSync Web-ACLs für Körper den Text ein. 8192 Geben Sie für Web-ACLs in CloudFront API Gateway, Amazon Cognito, App Runner oder Verified Access ein, wenn Sie die standardmäßige Körpergrößenbeschränkung verwenden. 16384 Geben Sie andernfalls die Körpergrößenbeschränkung ein, die Sie für Ihre Web-ACL definiert haben.
 - d. Wählen Sie für Oversize handling (Handhabung zu großer Inhalte) die Option Match (Übereinstimmung) aus.
4. Wählen Sie für Action (Aktion) die Option Block (Blockieren) aus.
5. Wählen Sie Regel hinzufügen aus.
6. Wenn Sie die Regel hinzugefügt haben, verschieben Sie sie auf der Seite Set rule priority (Regelpriorität festlegen) über alle Regeln oder Regelgruppen in der Web-ACL, die denselben Komponententyp untersuchen. Dadurch wird ihr eine niedrigere numerische Priorität zugewiesen, weshalb AWS WAF sie zuerst ausgewertet wird. Weitere Informationen finden Sie unter [Reihenfolge der Verarbeitung von Regeln und Regelgruppen in einer Web-ACL](#).

Musterabgleich mit regulären Ausdrücken in AWS WAF

AWS WAF unterstützt die von der PCRE-Bibliothek `libpcre` verwendete Mustersyntax. Die Bibliothek ist unter [PCRE - Perl Compatible Regular Expressions](#) (Perl-kompatible reguläre Ausdrücke) dokumentiert.

AWS WAF unterstützt nicht alle Konstrukte der Bibliothek. Zum Beispiel unterstützt es einige Nullbreiten-Assertionen, aber nicht alle. Wir haben keine umfassende Liste der unterstützten Konstrukte. Wenn Sie jedoch ein ungültiges Regex-Muster angeben oder nicht unterstützte Konstrukte verwenden, meldet die AWS WAF API einen Fehler.

AWS WAF unterstützt die folgenden PCRE-Muster nicht:

- Rückverweise und Erfassung von Teilausdrücken
- Subroutine-Referenzen und rekursive Muster
- Bedingungsmuster
- Rückverfolgung von Kontrollverben
- Die `\C` Einbyte-Richtlinie
- Die `\R`-Newline-Match-Richtlinie
- Die `\K`-Start der Match-Reset-Richtlinie
- Callouts und eingebetteter Code
- Atomic Grouping und possessive Quantifizierer

IP-Sätze und Regex-Mustersätze in AWS WAF

AWS WAF speichert einige komplexere Informationen in Gruppen, die Sie verwenden, indem Sie in Ihren Regeln auf sie verweisen. Jedes dieser Sets hat einen Namen und erhält bei der Erstellung einen Amazon-Resource-Namen (ARN). Sie können diese Sets aus Ihren Regelanweisungen verwalten und über die Konsolen-Navigation auf sie zugreifen und sie so verwalten.

Temporäre Inkonsistenzen bei Aktualisierungen

Wenn Sie eine Web-ACL oder andere AWS WAF Ressourcen erstellen oder ändern, dauert es nicht lange, bis die Änderungen in allen Bereichen, in denen die Ressourcen gespeichert sind, übernommen werden. Die Übertragungszeit kann zwischen einigen Sekunden und mehreren Minuten liegen.

Im Folgenden finden Sie Beispiele für temporäre Inkonsistenzen, die Ihnen bei der Übertragung von Änderungen möglicherweise auffallen:

- Wenn Sie nach der Erstellung einer Web-ACL versuchen, sie einer Ressource zuzuordnen, wird möglicherweise eine Ausnahme angezeigt, die darauf hinweist, dass die Web-ACL nicht verfügbar ist.
- Nachdem Sie einer Web-ACL eine Regelgruppe hinzugefügt haben, gelten die neuen Regelgruppenregeln möglicherweise in einem Bereich, in dem die Web-ACL verwendet wird, und nicht in einem anderen.
- Nachdem Sie eine Regelaktionseinstellung geändert haben, sehen Sie möglicherweise an einigen Stellen die alte Aktion und an anderen die neue Aktion.
- Nachdem Sie einem IP-Set, das in einer Sperrregel verwendet wird, eine IP-Adresse hinzugefügt haben, wird die neue Adresse möglicherweise in einem Bereich blockiert, während sie in einem anderen weiterhin zulässig ist.

Themen

- [Erstellen und verwalten eines IP-Sets](#)
- [Erstellen und Verwalten eines Regex-Mustersatzes](#)

Erstellen und verwalten eines IP-Sets

Ein IP-Set stellt eine Sammlung von IP-Adressen und IP-Adressbereichen bereit, die Sie in einer Regelanweisung gemeinsam verwenden möchten. IP-Sets sind AWS Ressourcen.

Um einen IP-Satz in einer Web-ACL oder Regelgruppe zu verwenden, erstellen Sie zunächst eine AWS Ressource IPSet mit Ihren Adressspezifikationen. Dann referenzieren Sie den Satz, wenn Sie eine IP-Regelanweisung für einen Regelsatz zu einer Web-ACL oder Regelgruppe hinzufügen.

Themen

- [Erstellen eines IP-Sets](#)
- [Verwenden eines IP-Sets in einer Regelgruppe oder Web-ACL](#)
- [Bearbeiten eines IP-Sets](#)
- [Löschen eines IP-Sets](#)

Erstellen eines IP-Sets

Gehen Sie wie in diesem Abschnitt beschrieben vor, um ein neues IP-Set zu erstellen.

Note

Zusätzlich zur Vorgehensweise in diesem Abschnitt haben Sie die Möglichkeit, ein neues IP-Set hinzuzufügen, wenn Sie eine IP-Match-Regel zu Ihrer Web-ACL oder Regelgruppe hinzufügen. Wenn Sie diese Option wählen, müssen Sie dieselben Einstellungen vornehmen wie bei diesem Verfahren.

So erstellen Sie ein IP-Set

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich IP-Sets und dann Create IP set (IP-Set erstellen).
3. Geben Sie einen Namen und eine Beschreibung für das IP-Set ein. Sie werden diesen verwenden, um einen Satz zu identifizieren, wenn Sie diesen verwenden möchten.

Note

Sie können den Namen nach der Erstellung des IP-Sets nicht mehr ändern.

4. Wählen Sie unter Region die Option Global (CloudFront) oder die Region aus, in der Sie den IP-Satz speichern möchten. Sie können regionale IP-Sätze nur in Web-ACLs verwenden, die regionale Ressourcen schützen. Um eine IP-Adresse in Web-ACLs zu verwenden, die CloudFront Amazon-Distributionen schützen, müssen Sie Global () CloudFront verwenden.
5. Wählen Sie für IP-Version die Version aus, die Sie verwenden möchten.
6. Geben Sie im Textfeld IP-Adressen eine IP-Adresse oder einen IP-Adressbereich pro Zeile in CIDR-Notation ein. AWS WAF unterstützt alle IPv4- und IPv6-CIDR-Bereiche mit Ausnahme von `/0`. Weitere Informationen zu CIDR-Notationen finden Sie im Wikipedia-Artikel [Classless Inter-Domain Routing](#).

Hier sind einige Beispiele:

- Für die IPv4-Adresse 192.0.2.44 geben Sie 192.0.2.44/32 ein.

- Um die IPv6-Adresse 2620:0:2 d 0:200:0:0:0:0 anzugeben, geben Sie 2620:0:2 d 0:200:0:0:0:0 /128 ein.
 - Für den Bereich von IPv4-Adressen von 192.0.2.0 bis 192.0.2.255 geben Sie 192.0.2.0/24 ein.
 - Um den Bereich der IPv6-Adressen von 2620:0:2d0:200:0:0:0:0 to 2620:0:2d0:200:ffff:ffff:ffff:ffff anzugeben, geben Sie 2620:0:2d0:200::/64 ein.
7. Überprüfen Sie die Einstellungen für das IP-Set und wählen Sie Create IP set (IP-Set erstellen).

Verwenden eines IP-Sets in einer Regelgruppe oder Web-ACL

Um ein IP-Set zu verwenden, fügen Sie eine Regelanweisung hinzu, die auf die Regelgruppe oder Web-ACL verweist, in der sie diese benötigen. Weitere Informationen finden Sie unter [IP-Set-Übereinstimmungsregelung](#).

Bearbeiten eines IP-Sets

Um IP-Adressen oder IP-Adressbereiche zu einem IP-Set hinzuzufügen oder zu entfernen oder seine Beschreibung zu ändern, führen Sie die folgende Vorgehensweise aus.

So bearbeiten Sie ein IP-Set

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich IP-Sets.
3. Wählen Sie das IP-Set, das Sie bearbeiten möchten, und wählen Sie Edit (Bearbeiten).
4. Ändern Sie die IP-Version und -Adressen nach Bedarf. Im Textfeld IP-Adressen müssen Sie eine IP-Adresse oder einen IP-Adressbereich pro Zeile in CIDR-Notation angeben. AWS WAF unterstützt alle IPv4- und IPv6-CIDR-Bereiche mit Ausnahme von. /0 Weitere Informationen zu CIDR-Notationen finden Sie im Wikipedia-Artikel [Classless Inter-Domain Routing](#). Geben Sie für Adressen eine IP-Adresse oder einen IP-Adressbereich pro Zeile in CIDR-Notation ein.

Hier sind einige Beispiele:

- Für die IPv4-Adresse 192.0.2.44 geben Sie 192.0.2.44/32 ein.
- Um die IPv6-Adresse 2620:0:2 d 0:200:0:0:0:0 anzugeben, geben Sie 2620:0:2 d 0:200:0:0:0:0 /128 ein.
- Für den Bereich von IPv4-Adressen von 192.0.2.0 bis 192.0.2.255 geben Sie 192.0.2.0/24 ein.

- Um den Bereich der IPv6-Adressen von 2620:0:2d0:200:0:0:0:0 to 2620:0:2d0:200:ffff:ffff:ffff:ffff anzugeben, geben Sie 2620:0:2d0:200::/64 ein.

5. Wählen Sie Save Changes.

Löschen eines IP-Sets

Befolgen Sie die Anweisungen in diesem Abschnitt, um ein referenziertes Set zu löschen.

Löschen von referenzierten Sets oder Regelgruppen

Wenn Sie eine Entität löschen, die Sie in einer Web-ACL verwenden können, z. B. einen IP-Satz, einen Regex-Mustersatz oder eine Regelgruppe, wird AWS WAF überprüft, ob die Entität derzeit in einer Web-ACL verwendet wird. Wenn es feststellt, dass es verwendet wird, werden Sie AWS WAF gewarnt. AWS WAF kann fast immer feststellen, ob eine Web-ACL auf eine Entität verweist. In seltenen Fällen ist dies jedoch nicht möglich. Wenn Sie sicherstellen müssen, dass die Entität derzeit nicht verwendet, überprüfen Sie sie in den Web-ACLs, bevor Sie sie löschen. Wenn es sich bei der Entität um ein referenziertes Set handelt, stellen Sie sicher, dass keine Regelgruppen es verwenden.

So löschen Sie ein IP-Set

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich IP-Sets.
3. Wählen Sie das IP-Set, das Sie löschen möchten, und wählen Sie Delete (Löschen).

Erstellen und Verwalten eines Regex-Mustersatzes

Ein Regex-Mustersatz stellt eine Sammlung von regulären Ausdrücken zur Verfügung, die Sie zusammen in einer Regelanweisung verwenden möchten. Regex-Mustersätze sind AWS Ressourcen.

Um einen Regex-Mustersatz in einer Web-ACL oder Regelgruppe zu verwenden, erstellen Sie zunächst eine AWS Ressource `RegexPatternSet` mit Ihren Regex-Musterspezifikationen. Dann referenzieren Sie den Satz, wenn Sie eine Regex-Regelanweisung für einen Regelsatz zu einer Web-ACL oder Regelgruppe hinzufügen. Ein `Regex`-Mustersatz muss mindestens ein `Regex`-Muster enthalten.

Wenn Ihr Regex-Mustersatz mehr als ein Regex-Muster enthält, wird bei dessen Verwendung in einer Regel der Musterabgleich mit einem OR-Logik kombiniert. Das heißt, eine Webanforderung stimmt mit der Musterregelanzweisung überein, wenn die Anforderungskomponente mit einem der Muster im Satz übereinstimmt.

AWS WAF unterstützt mit einigen Ausnahmen die von der PCRE-Bibliothek verwendete Mustersyntax. `libpcre` Die Bibliothek ist unter [PCRE - Perl Compatible Regular Expressions](#) (Perl-kompatible reguläre Ausdrücke) dokumentiert. Hinweise zur AWS WAF Unterstützung finden Sie unter [Musterabgleich mit regulären Ausdrücken in AWS WAF](#).

Themen

- [Löschen eines Regex-Mustersatzes](#)
- [Verwenden eines Regex-Mustersatzes in einer Regelgruppe oder Web-ACL](#)
- [Löschen eines Regex-Mustersatzes](#)

Löschen eines Regex-Mustersatzes

Gehen Sie wie in diesem Abschnitt beschrieben vor, um einen neuen RegEx-Mustersatz zu erstellen.

So erstellen Sie einen RegEx-Mustersatz

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich Regex pattern sets (Regex-Mustersätze) und dann Create regex pattern set (Regex-Mustersatz erstellen).
3. Geben Sie einen Namen und eine Beschreibung für den Regex-Mustersatz ein. Sie werden diesen verwenden, um einen Satz zu identifizieren, wenn Sie diesen verwenden möchten.

Note

Sie können den Namen nicht mehr ändern, nachdem Sie den RegEx-Mustersatz erstellt haben.

4. Wählen Sie für Region die Option Global (CloudFront) oder die Region aus, in der Sie den Regex-Mustersatz speichern möchten. Sie können regionale Regex-Mustersätze nur in Web-ACLs verwenden, die regionale Ressourcen schützen. Um ein Regex-Muster zu verwenden,

das in Web-ACLs zum Schutz von CloudFront Amazon-Distributionen festgelegt ist, müssen Sie Global () verwenden. CloudFront

5. Geben Sie im Textfeld Regular expressions (Reguläre Ausdrücke) ein RegEx-Muster pro Zeile ein.

Der reguläre Ausdruck `I[a@]mAB[a@]dRequest` entspricht beispielsweise den folgenden Zeichenfolgen: `IamABadRequest`, `IamAB@dRequest`, `I@mABadRequest` und `I@mAB@dRequest`.

AWS WAF unterstützt mit einigen Ausnahmen die von der PCRE-Bibliothek verwendete Mustersyntax. `libpcre` Die Bibliothek ist unter [PCRE - Perl Compatible Regular Expressions](#) (Perl-kompatible reguläre Ausdrücke) dokumentiert. Hinweise zur AWS WAF Unterstützung finden Sie unter [Musterabgleich mit regulären Ausdrücken in AWS WAF](#).

6. Überprüfen Sie die Einstellungen für den Regex-Mustersatz und wählen Sie Create regex pattern set (Regex-Mustersatz erstellen).

Verwenden eines Regex-Mustersatzes in einer Regelgruppe oder Web-ACL

Um einen Regex-Mustersatz in einer Regelgruppe oder Web-ACL zu verwenden, wählen Sie in der Konsole beim Hinzufügen oder Aktualisieren der Regeln in Ihrer Regelgruppe oder Web-ACL in der Regel-Builder-Oberfläche für Request Option (Anforderungsoption) die Anforderungskomponente aus, die Sie mit Ihrem Mustersatz vergleichen möchten. Wählen Sie Match type (Übereinstimmungstyp) > String match condition (Zeichenfolgen-Übereinstimmungsbedingung) > Matches pattern from regular expression (Übereinstimmung des Musters aus dem regulären Ausdruck) aus. Wählen Sie dann den Namen des Regex-Mustersatzes aus, den Sie verwenden möchten.

Löschen eines Regex-Mustersatzes

Befolgen Sie die Anweisungen in diesem Abschnitt, um ein referenziertes Set zu löschen.

Löschen von referenzierten Sets oder Regelgruppen

Wenn Sie eine Entität löschen, die Sie in einer Web-ACL verwenden können, z. B. einen IP-Satz, einen Regex-Mustersatz oder eine Regelgruppe, wird AWS WAF überprüft, ob die Entität derzeit in einer Web-ACL verwendet wird. Wenn es feststellt, dass es verwendet wird, werden Sie AWS WAF gewarnt. AWS WAF kann fast immer feststellen, ob eine Web-ACL auf eine Entität verweist. In seltenen Fällen ist dies jedoch nicht möglich. Wenn Sie sicherstellen müssen, dass die Entität derzeit

nicht verwendet, überprüfen Sie sie in den Web-ACLs, bevor Sie sie löschen. Wenn es sich bei der Entität um ein referenziertes Set handelt, stellen Sie sicher, dass keine Regelgruppen es verwenden.

So löschen Sie einen RegEx-Mustersatz

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich Regex pattern sets (Regex-Mustersätze).
3. Wählen Sie den zu löschenden Regex-Mustersatz aus und wählen Sie Delete (Löschen).

Benutzerdefinierte Webanforderungen und Antworten in AWS WAF

Sie können Ihren AWS WAF Regelaktionen und Standard-Web-ACL-Aktionen ein benutzerdefiniertes Verhalten bei der Verarbeitung von Webanfragen und Antworten hinzufügen. Ihre benutzerdefinierten Einstellungen werden immer dann angewendet, wenn die Aktion angewendet wird, der sie zugeordnet sind.

Sie können Webanforderungen und Antworten auf folgende Arten anpassen:

- Mit Challenge Aktionen AllowCount, CAPTCHA, und können Sie benutzerdefinierte Header in die Webanforderung einfügen. Wenn AWS WAF die Webanforderung an die geschützte Ressource weiterleitet, enthält die Anforderung die gesamte ursprüngliche Anforderung sowie die benutzerdefinierten Header, die Sie eingefügt haben. Wendet die Anpassung für die Challenge Aktionen CAPTCHA und AWS WAF nur an, wenn die Anfrage die CAPTCHA- oder Challenge-Token-Prüfung besteht.
- Mit Block Aktionen können Sie eine vollständige benutzerdefinierte Antwort mit Antwortcode, Headern und Text definieren. Die geschützte Ressource beantwortet die Anfrage mit der benutzerdefinierten Antwort von AWS WAF. Ihre benutzerdefinierte Antwort ersetzt die Block Standardaktionsantwort von 403 (Forbidden).

Anpassbare Aktionseinstellungen

Sie können eine benutzerdefinierte Anforderung oder Antwort angeben, wenn Sie die folgenden Aktionseinstellungen definieren:

- Regelaktion. Weitere Informationen finden Sie unter [Regelaktion](#).

- Standardaktion für eine Web-ACL. Weitere Informationen finden Sie unter [Die Web-ACL-Standardaktion](#).

Nicht anpassbare Aktionseinstellungen

Sie können keine benutzerdefinierte Anforderungsbehandlung in der Überschreibungsaktion für eine Regelgruppe angeben, die Sie in einer Web-ACL verwenden. Siehe [Auswertung von Web-ACL-Regeln und -Regelgruppen](#). Weitere Informationen finden Sie auch unter [Verwaltete Regelgruppenanweisung](#) und [Regelgruppenanweisung](#).

Temporäre Inkonsistenzen bei Updates

Wenn Sie eine Web-ACL oder andere AWS WAF Ressourcen erstellen oder ändern, dauert es nicht lange, bis die Änderungen in allen Bereichen, in denen die Ressourcen gespeichert sind, übernommen werden. Die Übertragungszeit kann zwischen einigen Sekunden und mehreren Minuten liegen.

Im Folgenden finden Sie Beispiele für temporäre Inkonsistenzen, die Ihnen bei der Übertragung von Änderungen möglicherweise auffallen:

- Wenn Sie nach der Erstellung einer Web-ACL versuchen, sie einer Ressource zuzuordnen, wird möglicherweise eine Ausnahme angezeigt, die darauf hinweist, dass die Web-ACL nicht verfügbar ist.
- Nachdem Sie einer Web-ACL eine Regelgruppe hinzugefügt haben, gelten die neuen Regelgruppenregeln möglicherweise in einem Bereich, in dem die Web-ACL verwendet wird, und nicht in einem anderen.
- Nachdem Sie eine Regelaktionseinstellung geändert haben, sehen Sie möglicherweise an einigen Stellen die alte Aktion und an anderen die neue Aktion.
- Nachdem Sie einem IP-Satz, der in einer Sperrregel verwendet wird, eine IP-Adresse hinzugefügt haben, wird die neue Adresse möglicherweise in einem Bereich blockiert, während sie in einem anderen weiterhin zulässig ist.

Beschränkungen für Ihre Verwendung von benutzerdefinierten Anforderungen und Antworten

AWS WAF definiert maximale Einstellungen für Ihre Verwendung von benutzerdefinierten Anfragen und Antworten. Beispielsweise eine maximale Anzahl von Anforderungsheadern pro Web-ACL oder Regelgruppe und eine maximale Anzahl von benutzerdefinierten Headern für eine einzelne benutzerdefinierte Antwortdefinition. Weitere Informationen finden Sie unter [AWS WAF Kontingente](#).

Themen

- [Benutzerdefinierte Anforderungsheader-Einfügungen für nicht blockierende Aktionen](#)
- [Benutzerdefinierte Antworten für Block Aktionen](#)
- [Unterstützte Statuscodes für benutzerdefinierte Antwort](#)

Benutzerdefinierte Anforderungsheader-Einfügungen für nicht blockierende Aktionen

Sie können anweisen AWS WAF, benutzerdefinierte Header in die ursprüngliche HTTP-Anfrage einzufügen, wenn eine Regelaktion die Anfrage nicht blockiert. Mit dieser Option fügen Sie der Anfrage nur etwas hinzu. Sie können keinen Teil der ursprünglichen Anforderung ändern oder ersetzen. Zu den Anwendungsfällen für das Einfügen von benutzerdefinierten Headern gehört es, einer Downstream-Anwendung zu signalisieren, die Anforderung auf der Grundlage der eingefügten Header anders zu verarbeiten, und die Anforderung zur Analyse zu kennzeichnen.

Diese Option gilt für die Regelaktionen Allow, CountCAPTCHA, und Challenge und für Web-ACL-Standardaktionen, die auf eingestellt sind Allow. Weitere Informationen zu Regelaktionen unter [Regelaktion](#). Weitere Informationen zu standardmäßigen Web-ACL-Aktionen finden Sie unter [Die Web-ACL-Standardaktion](#).

Benutzerdefinierte Anforderungs-Header-Namen

AWS WAF stellt allen eingefügten Anforderungsheadern ein Präfix `x-amzn-waf-`, um Verwechslungen mit den Headern zu vermeiden, die bereits in der Anfrage enthalten sind. Wenn Sie beispielsweise den Header-Namen `angebensample`, wird der Header AWS WAF eingefügt. `x-amzn-waf-sample`

Header mit demselben Namen

Wenn die Anforderung bereits über einen Header mit demselben Namen verfügt, der gerade eingefügt AWS WAF wird, wird der Header AWS WAF überschrieben. Wenn Sie also in mehreren Regeln Header mit identischen Namen definieren, wird die Kopfzeile bei der letzten Regel hinzugefügt, die die Anforderung überprüft und eine Übereinstimmung findet. Die vorherigen Regeln würden dies nicht tun.

Benutzerdefinierte Header mit nicht beendenden Regelaktionen

Im Gegensatz zur Allow Aktion stoppt die Count Aktion nicht die Verarbeitung AWS WAF der Webanforderung mithilfe der übrigen Regeln in der Web-ACL. Auch wenn CAPTCHA Challenge

festgestellt wird, dass das Anforderungstoken gültig ist, beenden AWS WAF diese Aktionen nicht die Verarbeitung der Webanforderung. Wenn Sie also benutzerdefinierte Header mithilfe einer Regel mit einer dieser Aktionen einfügen, fügen nachfolgende Regeln möglicherweise auch benutzerdefinierte Header ein. Weitere Informationen zum Verhalten von Regelaktionen finden Sie unter [Regelaktion](#)

Angenommen die folgenden Regeln wurden mit der angezeigten Priorität festgelegt:

1. RegelA mit einer Count Aktion und einem benutzerdefinierten Header namens `RuleAHeader`.
2. RuleB mit einer Allow Aktion und einem benutzerdefinierten Header namens `RuleBHeader`

Wenn eine Anfrage sowohl mit RuleA als auch mit RuleB übereinstimmt, AWS WAF fügt die Header ein `x-amzn-waf-RuleAHeader` und `x-amzn-waf-RuleBHeader` leitet die Anfrage dann an die geschützte Ressource weiter.

AWS WAF fügt benutzerdefinierte Header in eine Webanforderung ein, wenn die Überprüfung der Anfrage abgeschlossen ist. Wenn Sie also die benutzerdefinierte Anforderungsbehandlung mit einer Regel verwenden, für die die Aktion auf festgelegt ist `Count`, werden die benutzerdefinierten Header, die Sie hinzufügen, nicht durch nachfolgende Regeln überprüft.

Beispiel: Benutzerdefinierte Anforderungsbehandlung

Sie definieren die benutzerdefinierte Anforderungsbehandlung für die Aktion einer Regel oder für die Standardaktion einer Web-ACL. Die folgende Auflistung zeigt den JSON-Code für die benutzerdefinierte Behandlung, die der Standardaktion für eine Web-ACL hinzugefügt wurde.

```
{
  "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"
}
}
```

Benutzerdefinierte Antworten für Block Aktionen

Sie können anweisen AWS WAF , für Regelaktionen oder Web-ACL-Standardaktionen, die auf eingestellt sind, eine benutzerdefinierte HTTP-Antwort zurück an den Client zu Block senden. Weitere Informationen zu Regelaktionen unter [Regelaktion](#). Weitere Informationen zu standardmäßigen Web-ACL-Aktionen finden Sie unter [Die Web-ACL-Standardaktion](#).

Wenn Sie die benutzerdefinierte Antwortbehandlung für eine Block Aktion definieren, definieren Sie den Statuscode, die Header und den Antworttext. Eine Liste der Statuscodes, die Sie zusammen verwenden können AWS WAF, finden Sie im folgenden Abschnitt. [Unterstützte Statuscodes für benutzerdefinierte Antwort](#)

Anwendungsfälle

Zu den Anwendungsfällen für benutzerdefinierte Antworten gehören:

- Senden eines nicht standardmäßigen Statuscodes an den Client zurück
- Senden benutzerdefinierter Antwortheader zurück an den Client. Sie können einen beliebigen Header-Namen angeben, mit Ausnahme content-type von.
- Senden einer statischen Fehlerseite an den Client zurück
- Umleiten des Clients auf eine andere URL Dazu geben Sie einen der 3xx-Umleitungsstatuscodes wie 301 (Moved Permanently) oder 302 (Found) und dann einen neuen Header mit dem Namen Location mit der neuen URL an.

Interaktion mit Antworten, die Sie in Ihrer geschützten Ressource definieren

Benutzerdefinierte Antworten, die Sie für die AWS WAF Block Aktion angeben, haben Vorrang vor allen Antwortspezifikationen, die Sie in Ihrer geschützten Ressource definieren.

Der Hostdienst für die AWS Ressource, mit der Sie schützen, ermöglicht AWS WAF möglicherweise eine benutzerdefinierte Antwortbehandlung für Webanfragen. Beispiele sind unter anderem:

- Bei Amazon CloudFront können Sie die Fehlerseite anhand des Statuscodes anpassen. Weitere Informationen finden Sie unter [Generieren benutzerdefinierter Fehlerantworten](#) im Amazon CloudFront Developer Guide.
- Mit Amazon API Gateway können Sie den Antwort- und Statuscode für Ihr Gateway definieren. Weitere Informationen finden Sie unter [Gateway-Antworten in API Gateway](#) im Entwicklerhandbuch für Amazon API Gateway.

Sie können AWS WAF benutzerdefinierte Antworteinstellungen nicht mit benutzerdefinierten Antworteinstellungen in der geschützten AWS Ressource kombinieren. Die Antwortspezifikation für jede einzelne Webanforderung stammt entweder vollständig von AWS WAF oder vollständig von der geschützten Ressource.

Für AWS WAF blockierte Webanfragen ist im Folgenden die Rangfolge aufgeführt.

1. AWS WAF benutzerdefinierte Antwort — Wenn für die AWS WAF Block Aktion eine benutzerdefinierte Antwort aktiviert ist, sendet die geschützte Ressource die konfigurierte benutzerdefinierte Antwort zurück an den Client. Alle Antworteinstellungen, die Sie möglicherweise in der geschützten Ressource selbst definiert haben, haben keine Auswirkungen.
2. Benutzerdefinierte Antwort, die in der geschützten Ressource definiert ist – Wenn für die geschützte Ressource benutzerdefinierte Antworteinstellungen angegeben wurden, verwendet die geschützte Ressource diese Einstellungen für die Antwort an den Client.
3. AWS WAF BlockStandardantwort — Andernfalls antwortet die geschützte Ressource dem Client mit der AWS WAF Block Standardantwort 403 (Forbidden).

Bei Webanfragen, die dies AWS WAF zulassen, bestimmt Ihre Konfiguration der geschützten Ressource die Antwort, die an den Client zurückgesendet wird. Sie können die Antworteinstellungen AWS WAF für zulässige Anfragen nicht konfigurieren. Die einzige Anpassung, die Sie AWS WAF für zulässige Anfragen konfigurieren können, ist das Einfügen von benutzerdefinierten Headern in die ursprüngliche Anfrage, bevor die Anfrage an die geschützte Ressource weitergeleitet wird. Diese Option wird im vorherigen Abschnitt ([Benutzerdefinierte Anforderungsheader-Einfügungen für nicht blockierende Aktionen](#)) beschrieben.

Benutzerdefinierte Antwort-Header

Sie können einen beliebigen Header-Namen angeben, mit Ausnahme `content-type` von.

Benutzerdefinierte Antworttexte

Sie definieren den Text einer benutzerdefinierten Antwort im Kontext der Web-ACL oder Regelgruppe, in der Sie sie verwenden möchten. Nachdem Sie einen benutzerdefinierten Antworttext definiert haben, können Sie ihn per Verweis an einer anderen Stelle in der Web-ACL oder Regelgruppe verwenden, in der Sie ihn erstellt haben. In den einzelnen Block Aktionseinstellungen verweisen Sie auf den benutzerdefinierten Text, den Sie verwenden möchten, und definieren den Statuscode und die Kopfzeile der benutzerdefinierten Antwort.

Wenn Sie eine benutzerdefinierte Antwort in der Konsole erstellen, können Sie aus Antworttexten auswählen, die Sie bereits definiert haben, oder Sie können einen neuen Text erstellen. Außerhalb der Konsole definieren Sie Ihre benutzerdefinierten Antworttexte auf Web-ACL- oder Regelgruppenebene und referenzieren sie dann aus den Aktionseinstellungen innerhalb der Web-ACL oder Regelgruppe. Dies wird im Beispiel-JSON-Code im folgenden Abschnitt gezeigt.

Beispiel: Benutzerdefinierte Antwort

Im folgenden Beispiel wird der JSON-Code für eine Regelgruppe mit benutzerdefinierten Antworteinstellungen aufgeführt. Der benutzerdefinierte Antworttext wird für die gesamte Regelgruppe definiert und dann durch Schlüssel in der Regelaktion referenziert.

```
{
  "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
}
}
```

Unterstützte Statuscodes für benutzerdefinierte Antwort

Ausführliche Informationen zu HTTP-Statuscodes finden Sie unter [Statuscodes](#) der Internet Engineering Task Force (IETF) und [Liste der HTTP-Statuscodes](#) auf Wikipedia.

Im Folgenden sind die HTTP-Statuscodes aufgeführt, die benutzerdefinierte Antworten AWS WAF unterstützen.

- 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 Labels auf Webanfragen

Bei einem Label handelt es sich um Metadaten, die einer Webanfrage durch eine entsprechende Regel hinzugefügt wurden. Wenn eine Regel mit einer Webanforderung übereinstimmt und für die Regel Bezeichnungen angegeben sind, werden diese der Anfrage AWS WAF hinzugefügt. Die Labels bleiben in der Anfrage verfügbar, bis die Web-ACL-Evaluierung abgeschlossen ist. Sie können auf Labels in Regeln zugreifen, die später in der Web-ACL-Evaluierung ausgeführt werden, indem Sie eine Label Match-Anweisung verwenden. Details hierzu finden Sie unter [Regelanweisung für Bezeichnungsübereinstimmung](#).

Labels in Webanfragen generieren CloudWatch Amazon-Labelmetriken. Eine Liste der Metriken und Dimensionen finden Sie unter [Kennzeichnen Sie Metriken und Dimensionen](#). Informationen zum Zugriff auf Metriken und Metrikzusammenfassungen über CloudWatch und über die AWS WAF Konsole finden Sie unter [Überwachung und Tuning](#).

Anwendungsfälle kennzeichnen

Zu den häufigsten Anwendungsfällen für AWS WAF Etiketten gehören:

- Evaluierung einer Webanforderung anhand mehrerer Regelanweisungen, bevor Maßnahmen für die Anfrage ergriffen werden — Nachdem eine Übereinstimmung mit einer Regel in einer Web-ACL gefunden wurde, wird die Anfrage anhand der Web-ACL AWS WAF weiter ausgewertet, sofern die Regelaktion die Web-ACL-Evaluierung nicht beendet. Sie können Labels verwenden, um Informationen aus mehreren Regeln auszuwerten und zu sammeln, bevor Sie entscheiden, die Anfrage zuzulassen oder zu blockieren. Ändern Sie dazu die Aktionen für Ihre vorhandenen Regeln in Count und konfigurieren Sie sie so, dass den entsprechenden Anfragen Labels hinzugefügt

werden. Fügen Sie dann eine oder mehrere neue Regeln hinzu, die nach Ihren anderen Regeln ausgeführt werden sollen, und konfigurieren Sie sie so, dass sie die Labels auswerten und die Anfragen entsprechend den Label-Match-Kombinationen verwalten.

- Verwaltung von Webanfragen nach geografischer Region — Sie können nur die geografische Vergleichsregel verwenden, um Webanfragen nach Herkunftsland zu verwalten. Um den Standort bis auf Regionsebene zu optimieren, verwenden Sie die Geo-Match-Regel mit einer Count Aktion, gefolgt von einer Label-Abgleichsregel. Informationen zur Geo-Match-Regel finden Sie unter [Anweisung für Regel zur geographischen Übereinstimmung](#).
- Wiederverwenden von Logik über mehrere Regeln hinweg – Wenn Sie dieselbe Logik in mehreren Regeln wiederverwenden müssen, können Sie die Logik mit Hilfe von Bezeichnungen aus einer Quelle beziehen und nur die Ergebnisse testen. Wenn Sie mehrere komplexe Regeln haben, die eine gemeinsame Teilmenge von verschachtelten Regelanweisungen verwenden, kann die Duplizierung des gemeinsamen Regelsatzes für Ihre komplexen Regeln zeitaufwendig und fehleranfällig sein. Mit Bezeichnungen können Sie eine neue Regel mit dem gemeinsamen Regelteilsatz erstellen, die übereinstimmende Anforderungen zählt und ihnen eine Bezeichnung hinzufügt. Sie fügen die neue Regel zu Ihrer Web-ACL hinzu, damit sie vor Ihren ursprünglichen komplexen Regeln ausgeführt wird. Dann ersetzen Sie in Ihren ursprünglichen Regeln den gemeinsamen Regelteilsatz durch eine einzelne Regel, die auf die Bezeichnung prüft.

Angenommen, Sie haben mehrere Regeln, die Sie nur auf Ihre Anmeldepfade anwenden möchten. Anstatt in jeder Regel dieselbe Logik zum Abgleich potenzieller Anmeldepfade anzugeben, können Sie eine einzige neue Regel implementieren, die diese Logik enthält. Die neue Regel fügt den übereinstimmenden Anforderungen eine Bezeichnung hinzu, um anzuzeigen, dass sich die Anforderung auf einem Anmeldepfad befindet. Geben Sie dieser neuen Regel in Ihrer Web-ACL eine niedrigere numerische Prioritätseinstellung als Ihren ursprünglichen Regeln, damit sie zuerst ausgeführt wird. Ersetzen Sie dann in Ihren ursprünglichen Regeln die gemeinsame Logik durch eine Überprüfung auf das Vorhandensein der Bezeichnung. Weitere Informationen zu Prioritätseinstellungen finden Sie unter [Reihenfolge der Verarbeitung von Regeln und Regelgruppen in einer Web-ACL](#).

- Erstellen von Ausnahmen von Regeln in Regelgruppen – Diese Option ist besonders nützlich für verwaltete Regelgruppen, die Sie nicht anzeigen oder ändern können. Viele Regeln für verwaltete Regelgruppen fügen übereinstimmenden Webanfragen Labels hinzu, um anzugeben, welche Regeln zutreffen, und um möglicherweise zusätzliche Informationen über die Übereinstimmung bereitzustellen. Wenn Sie eine Regelgruppe verwenden, die Bezeichnungen zu Anfragen hinzufügt, können Sie die Regelgruppenregeln überschreiben, um Treffer zu zählen, und dann eine Regel nach der Regelgruppe ausführen, die die Webanfrage auf der

Grundlage der Regelgruppenbezeichnungen bearbeitet. Alle von AWS verwalteten Regeln fügen übereinstimmenden Webanforderungen Bezeichnungen hinzu. Weitere Informationen erhalten Sie in den Regelbeschreibungen unter [AWS Liste der Regelgruppen für verwaltete Regeln](#).

- Verwenden von Label-Metriken zur Überwachung von Verkehrsmustern — Sie können auf Metriken für Labels zugreifen, die Sie über Ihre Regeln hinzufügen, und auf Metriken, die von allen verwalteten Regelgruppen hinzugefügt wurden, die Sie in Ihrer Web-ACL verwenden. Alle Regelgruppen für AWS verwaltete Regeln fügen den Webanfragen, die sie auswerten, Labels hinzu. Eine Liste der Label-Metriken und Dimensionen finden Sie unter [Kennzeichnen Sie Metriken und Dimensionen](#). Sie können über und über die ACL-Web-Seite in der AWS WAF Konsole auf Metriken CloudWatch und Metrikzusammenfassungen zugreifen. Weitere Informationen finden Sie unter [Überwachung und Tuning](#).

Funktionsweise von Bezeichnungen

Wenn eine Regel mit einer Webanforderung übereinstimmt und für die Regel Labels definiert sind, werden die Labels der Anfrage am Ende der Regelauswertung AWS WAF hinzugefügt. Regeln, die nach der entsprechenden Regel in der Web-ACL ausgewertet werden, können mit den Bezeichnungen übereinstimmen, die die Regel hinzugefügt hat.

Wer fügt Beschriftungen zu Anfragen hinzu

Die Web-ACL-Komponenten, die Anfragen auswerten, können den Anfragen Labels hinzufügen.

- Jede Regel, bei der es sich nicht um eine Referenzanweisung für eine Regelgruppe handelt, kann den entsprechenden Webanfragen Labels hinzufügen. Die Kennzeichnungskriterien sind Teil der Regeldefinition. Wenn eine Webanforderung der Regel entspricht, werden der Anfrage die Bezeichnungen der Regel AWS WAF hinzugefügt. Weitere Informationen finden Sie unter [the section called “Hinzufügen einer Bezeichnung”](#).
- Die Geo-Match-Regelanweisung fügt jeder Anfrage, die sie überprüft, Länder- und Regionskennzeichnungen hinzu, unabhängig davon, ob die Aussage zu einer Übereinstimmung führt. Weitere Informationen finden Sie unter [the section called “Geographische Übereinstimmung”](#).
- Die AWS verwalteten Regeln für AWS WAF alle fügen den Anfragen, die sie prüfen, Beschriftungen hinzu. Sie fügen einige Beschriftungen hinzu, die auf Regelübereinstimmungen in der Regelgruppe basieren, und sie fügen einige hinzu, die auf AWS Prozessen basieren, die von den verwalteten Regelgruppen verwendet werden, z. B. die Token-Kennzeichnung, die hinzugefügt wird, wenn Sie eine Regelgruppe zur intelligenten Abwehr von Bedrohungen

verwenden. Informationen zu den Bezeichnungen, die jede verwaltete Regelgruppe hinzufügt, finden Sie unter [the section called “AWS Liste der Regelgruppen für verwaltete Regeln”](#).

Wie AWS WAF verwaltet man Labels

AWS WAF fügt die Bezeichnungen der Regel zur Anfrage hinzu, wenn die Regel die Anfrage überprüft hat. Die Kennzeichnung ist, ähnlich wie die Aktion, Teil der Abgleichsaktivitäten einer Regel.

Bezeichnungen bleiben nicht mit der Webanforderung bestehen, nachdem die Auswertung durch die Web-ACL beendet wurde. Damit andere Regeln Abgleiche mit Bezeichnungen vornehmen können, die durch eine Ihrer Regeln hinzugefügt werden, darf Ihre Regelaktion die Auswertung der Webanforderung durch die Web-ACL nicht beenden. Die Regelaktion muss auf `CountCAPTCHA`, oder `gesetzt seinChallenge`. Wenn die Auswertung durch die Web-ACL nicht beendet wird, können nachfolgende Regeln in der Web-ACL ihre Kriterien für den Bezeichnungsabgleich auf die Anforderung anwenden. Weitere Informationen zu Regelaktionen unter [Regelaktion](#).

Wie greife ich während der Web-ACL-Evaluierung auf Labels zu

Nach dem Hinzufügen bleiben Labels in der Anfrage verfügbar, solange die Anfrage anhand der Web-ACL bewertet AWS WAF wird. Jede Regel in einer Web-ACL kann auf Labels zugreifen, die durch Regeln hinzugefügt wurden, die bereits in derselben Web-ACL ausgeführt wurden. Dazu gehören Regeln, die direkt in der Web-ACL definiert sind, und Regeln, die innerhalb von Regelgruppen definiert sind, die in der Web-ACL verwendet werden.

- Mithilfe der Anweisung „Label Match“ können Sie einen Abgleich mit einem Label in den Kriterien für die Anforderungsprüfung Ihrer Regel vornehmen. Sie können einen Abgleich mit jedem Etikett durchführen, das der Anfrage beigefügt ist. Details zur Anweisung finden Sie unter [Regelanweisung für Bezeichnungsübereinstimmung](#).
- Die geografische Zuordnung fügt Beschriftungen mit oder ohne Treffer hinzu. Sie sind jedoch erst verfügbar, nachdem die Web-ACL-Regel, die die Anweisung enthält, die Auswertung der Anfrage abgeschlossen hat.
 - Sie können nicht eine einzelne Regel, z. B. eine logische AND Aussage, verwenden, um eine Geo-Match-Anweisung gefolgt von einer Label-Match-Anweisung anhand der geografischen Beschriftungen auszuführen. Sie müssen die Label-Match-Anweisung in eine separate Regel einfügen, die nach der Regel ausgeführt wird, die die Geo-Match-Anweisung enthält.
 - Wenn Sie eine Geo-Match-Anweisung als Scopedown-Aussage innerhalb einer ratenbasierten Regelaussage oder einer Referenzaussage für verwaltete Regelgruppen verwenden, können die Bezeichnungen, die durch die Geo-Match-Anweisung hinzugefügt werden, nicht durch

die Anweisung der Regel überprüft werden, die sie enthält. Wenn Sie die geografische Kennzeichnung in einer ratenbasierten Regelaussage oder einer Regelgruppe überprüfen müssen, müssen Sie die Geo-Match-Anweisung in einer separaten Regel ausführen, die zuvor ausgeführt wird.

Wie greife ich außerhalb der Web-ACL-Evaluierung auf Labelinformationen zu

Labels werden nach Abschluss der Web-ACL-Evaluierung nicht in der Webanfrage gespeichert, sondern AWS WAF zeichnet Labelinformationen in den Protokollen und in Metriken auf.

- AWS WAF speichert CloudWatch Amazon-Metriken für die ersten 100 Labels auf jeder einzelnen Anfrage. Informationen zum Zugriff auf Label-Metriken finden Sie unter [Überwachung mit Amazon CloudWatch](#) und [Kennzeichnen Sie Metriken und Dimensionen](#).
- AWS WAF fasst die CloudWatch Label-Metriken in den Web-ACL-Traffic-Übersichts-Dashboards in der AWS WAF Konsole zusammen. Sie können auf jeder ACL-Web-Seite auf die Dashboards zugreifen. Weitere Informationen finden Sie unter [Dashboards zur Übersicht über den Web-ACL-Verkehr](#).
- AWS WAF zeichnet Labels in den Logs für die ersten 100 Labels einer Anfrage auf. Sie können Bezeichnungen zusammen mit der Regelaktion verwenden, um die Protokolle zu filtern, die AWS WAF aufzeichnet. Weitere Informationen finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).

Bei Ihrer Web-ACL-Auswertung können mehr als 100 Labels auf eine Webanfrage angewendet und diese mit mehr als 100 Labels abgeglichen werden. In den Logs und Metriken werden jedoch AWS WAF nur die ersten 100 Labels aufgezeichnet.

Bezeichnungssyntax- und Benennungsanforderungen

Eine Bezeichnung ist eine Zeichenfolge, die aus einem Präfix, optionalen Namespaces und einem Namen besteht. Die Komponenten von Bezeichnungen werden durch Doppelpunkte voneinander abgegrenzt. Für Bezeichnungen gelten die folgenden Anforderungen und Eigenschaften:

- Bei den Bezeichnungen muss die Groß- und Kleinschreibung beachtet werden.
- Jeder Bezeichnungs-Namespace oder Bezeichnungsname kann bis zu 128 Zeichen enthalten.
- Sie können bis zu fünf Namespaces in einer Beschriftung angeben.
- Komponenten von Bezeichnungen werden durch Doppelpunkte (:) voneinander abgegrenzt.

- Die folgenden reservierten Zeichenfolgen können Sie in den Namespaces oder Namen, die Sie für eine Bezeichnung angeben, nicht verwenden: `awsaf`, `aws`, `waf`, `rulegroup`, `webacl`, `regexpatternset`, `ipset` und `managed`.

Bezeichnungssyntax

Ein vollqualifiziertes Label hat ein Präfix, optionale Namespaces und einen Labelnamen. Das Präfix identifiziert die Regelgruppe oder den Web-ACL-Kontext der Regel, die die Beschriftung hinzugefügt hat. Namespaces können verwendet werden, um dem Label mehr Kontext hinzuzufügen. Der Labelname stellt die niedrigste Detailebene für ein Label dar. Er gibt häufig die spezifische Regel an, die das Label zur Anfrage hinzugefügt hat.

Das Bezeichnungspräfix variiert je nach Herkunft.

- **Deine Bezeichnungen** – Im Folgenden wird die vollständige Bezeichnungssyntax für Bezeichnungen angezeigt, die Sie in Ihren Web-ACL- und Regelgruppenregeln erstellen. Die Entitätstypen sind `rulegroup` und `webacl`.

```
awsaf:<entity owner account id>:<entity type>:<entity name>:<custom namespace>:...:<label name>
```

- **Bezeichnungs-Namespace-Präfix:** `awsaf:<entity owner account id>:<entity type>:<entity name>:`
- **Benutzerdefinierte Namespace-Ergänzungen:** `<custom namespace>:...:`

Wenn Sie eine Bezeichnung für eine Regel in einer Regelgruppe oder Web-ACL definieren, legen Sie die benutzerdefinierten Namespace-Zeichenfolgen und den Bezeichnungsnamen fest. Der Rest wird für Sie generiert von AWS WAF. AWS WAF setzt allen Bezeichnungen automatisch die Einstellungen für Konto `awsaf` und Web-ACL oder Regelgruppen-Entität voran.

- **Verwaltete Regelgruppenbezeichnungen** – Im Folgenden wird die vollständige Bezeichnungssyntax für Bezeichnungen dargestellt, die von Regeln in verwalteten Regelgruppen erstellt werden.

```
awsaf:managed:<vendor>:<rule group name>:<custom namespace>:...:<label name>
```

- **Bezeichnungs-Namespace-Präfix:** `awsaf:managed:<vendor>:<rule group name>:`
- **Benutzerdefinierte Namespace-Ergänzungen:** `<custom namespace>:...:`

Alle Regelgruppen mit AWS verwalteten Regeln fügen Labels hinzu. Informationen zu verwalteten Regelgruppen finden Sie unter [Verwaltete Regelgruppen](#).

- Labels aus anderen AWS Prozessen — Diese Prozesse werden von Regelgruppen mit AWS verwalteten Regeln verwendet, sodass Sie sehen, dass sie zu Webanfragen hinzugefügt werden, die Sie mithilfe verwalteter Regelgruppen auswerten. Im Folgenden wird die vollständige Bezeichnungssyntax für Bezeichnungen dargestellt, die von Prozessen erstellt werden, die von verwalteten Regelgruppen aufgerufen werden.

```
aws:waf:managed:<process>:<custom namespace>:...:<label name>
```

- Bezeichnungs-Namespace-Präfix: `aws:waf:managed:<process>:`
- Benutzerdefinierte Namespace-Ergänzungen: `<custom namespace>:...:`

Bezeichnungen dieses Typs werden für die verwalteten Regelgruppen aufgeführt, die den AWS -Prozess aufrufen. Informationen zu verwalteten Regelgruppen finden Sie unter [Verwaltete Regelgruppen](#).

Bezeichnungsbeispiele für Ihre Regeln

Die folgenden Bezeichnungsbeispiele werden durch Regeln in einer Regelgruppe mit dem Namen `testRules` definiert, die dem Konto `111122223333` angehört.

```
aws:waf:111122223333:rulegroup:testRules:testNS1:testNS2:LabelNameA
```

```
aws:waf:111122223333:rulegroup:testRules:testNS1:LabelNameQ
```

```
aws:waf:111122223333:rulegroup:testRules:LabelNameZ
```

Die folgende Auflistung zeigt eine beispielhafte Bezeichnungsspezifikation in JSON-Code. Diese Bezeichnungsnamen enthalten benutzerdefinierte Namespace-Zeichenfolgen vor dem endenden Bezeichnungsnamen.

```
Rule: {
  Name: "label_rule",
  Statement: {...}
  RuleLabels: [
    Name: "header:encoding:utf8",
```

```

    Name: "header:user_agent:firefox"
  ],
  Action: { Count: {} }
}

```

Note

Auf diese Art der Auflistung können Sie in der Konsole über den Regel-JSON-Editor zugreifen.

Wenn Sie die vorangehende Regel in derselben Regelgruppe und demselben Konto wie die vorangehenden Bezeichnungsbeispiele ausführen, würden die resultierenden, voll qualifizierten Bezeichnungen wie folgt lauten:

```
awsfaf:111122223333:rulegroup:testRules:header:encoding:utf8
```

```
awsfaf:111122223333:rulegroup:testRules:header:user_agent:firefox
```

Bezeichnungsbeispiele für verwaltete Regelgruppen

Im Folgenden finden Sie Beispiele für Labels aus Regelgruppen mit AWS verwalteten Regeln und Prozessen, die sie aufrufen.

```
awsfaf:managed:aws:core-rule-set:NoUserAgent_Header
```

```
awsfaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments
```

```
awsfaf:managed:aws:atp:aggregate:attribute:compromised_credentials
```

```
awsfaf:managed:token:accepted
```

Hinzufügen einer Bezeichnung zu übereinstimmenden Webanforderungen

Wenn Sie ein Label für eine Regel definieren, AWS WAF fügt das Label Anfragen hinzu, die der Regel entsprechen. Sie definieren ein Label in einer Regel, indem Sie die benutzerdefinierten Namespace-Zeichenfolgen und den Namen angeben, die an das Label-Namespace-Präfix angehängt werden sollen. AWS WAF leitet das Präfix aus dem Kontext ab, in dem Sie die Regel

definieren. Weitere Informationen dazu finden Sie in den Bezeichnungssyntaxinformationen unter [Bezeichnungssyntax- und Benennungsanforderungen](#).

Mit Ausnahme der folgenden Ausnahmen können Sie jeder Regel Labels hinzufügen. Ihre Labels AWS WAF werden jeder Webanfrage hinzugefügt, die der Rule Match-Anweisung entspricht:

- Ratenbasierte Regeln fügen Webanfragen nur Labels für die spezifische Aggregationsinstanz hinzu, solange für diese Instanz eine Ratenbegrenzung gilt. AWS WAF Weitere Informationen über ratenbasierte Regeln finden Sie unter [Ratenbasierte Regelanweisung](#).
- Sie können keine Bezeichnungen in Anweisungen verwenden, die auf Regelgruppen verweisen. Wenn Sie versuchen, einer Regelgruppen-Regelanweisung über die API eine Bezeichnung hinzuzufügen, löst der Vorgang eine Validierungsausnahme aus. Weitere Informationen zu diesen Anweisungstypen finden Sie unter [Verwaltete Regelgruppenanweisung](#) und [Regelgruppenanweisung](#).

WCUs – 1 WCU für alle 5 Bezeichnungen, die Sie in Ihren Web-ACL- oder Regelgruppenregeln definieren.

Wo zu finden

- Rule Builder in der Konsole – Unter den Einstellungen Action (Aktion) der Regel, unter Label (Bezeichnung).
- API-Datentyp – Rule RuleLabels

Abgleich mit einer Bezeichnung

Sie können eine Anweisung zum Abgleich von Bezeichnungen verwenden, um Webanforderungsbezeichnungen auszuwerten. Sie können einen Abgleich mit einer Bezeichnung vornehmen, wofür der Name der Bezeichnung erforderlich ist, oder mit einem Namespace, wofür eine Namespace-Spezifikation erforderlich ist. Sowohl für Label als auch für Namespace können Sie optional vorangehende Namespaces und das Präfix in Ihre Spezifikation aufnehmen. Allgemeine Informationen zu dieser Anweisungsart finden Sie unter [Regelanweisung für Bezeichnungsübereinstimmung](#).

Das Präfix einer Bezeichnung definiert den Kontext der Regelgruppe oder Web-ACL, in der die Regel der Bezeichnung definiert ist. Wenn in der Label-Match-Anweisung einer Regel das Präfix nicht in Ihrer Label- oder Namespace-Übereinstimmungszeichenfolge angegeben ist, wird das Präfix für die Label-Abgleichsregel AWS WAF verwendet.

- Bezeichnungen für Regeln, die direkt in einer Web-ACL definiert sind, haben ein Präfix, das den Web-ACL-Kontext angibt.
- Bezeichnungen für Regeln, die sich innerhalb einer Regelgruppe befinden, haben ein Präfix, das den Kontext der Regelgruppe angibt. Das kann Ihre eigene Regelgruppe sein oder eine Regelgruppe, die für Sie verwaltet wird.

Weitere Informationen dazu finden Sie in den Bezeichnungssyntaxinformationen unter [Bezeichnungssyntax- und Benennungsanforderungen](#).

Note

Einige verwaltete Regelgruppen fügen Bezeichnungen hinzu. Sie können diese über die API abrufen, indem Sie `DescribeManagedRuleGroup` aufrufen. Die Bezeichnungen werden in der Eigenschaft `AvailableLabels` in der Antwort aufgeführt.

Wenn Sie eine Regel abgleichen möchten, die sich in einem anderen Kontext befindet als der Kontext Ihrer Regel, müssen Sie das Präfix in Ihrer Abgleichszeichenfolge angeben. Wenn Sie beispielsweise einen Abgleich mit Bezeichnungen vornehmen möchten, die durch Regeln in einer verwalteten Regelgruppe hinzugefügt wurden, können Sie eine Regel in Ihre Web-ACL mit einer Anweisung zum Abgleich von Bezeichnungen hinzufügen, deren Abgleichszeichenfolge das Präfix der Regelgruppe gefolgt von Ihren zusätzlichen Abgleichskriterien angibt.

In der Abgleichszeichenfolge für die Anweisung für den Abgleich von Bezeichnungen geben Sie entweder eine Bezeichnung oder einen Namespace an:

- **Bezeichnung** – Die Bezeichnungsspezifikation für einen Abgleich besteht aus dem Endteil der Bezeichnung. Sie können eine beliebige Anzahl der zusammenhängenden Namespaces angeben, die unmittelbar vor dem Bezeichnungsnamen gefolgt vom Namen liegen. Sie können die vollqualifizierte Bezeichnung auch angeben, indem Sie die Spezifikation mit dem Präfix beginnen.

Beispielspezifikationen:

- `testNS1:testNS2:LabelNameA`
- `awsaf:managed:aws:managed-rule-set:testNS1:testNS2:LabelNameA`
- **Namespace** – Die Namespace-Spezifikation für einen Abgleich besteht aus einer zusammenhängenden Teilmenge der Bezeichnungsspezifikation mit Ausnahme des Namens. Sie können das Präfix und mindestens eine Namespace-Zeichenfolge einschließen.

Beispielspezifikationen:

- testNS1:testNS2:
- awswaf:managed:aws:managed-rule-set:testNS1:

Beispiele für Bezeichnungsabgleich

Dieser Abschnitt enthält Beispiele für Abgleichsspezifikationen, für die Bezeichnungs-Abgleichsregelanweisung.

Note

Diese JSON-Einträge wurden in der Konsole erstellt, indem eine Regel zu einer Web-ACL mit den Spezifikationen für den Bezeichnungsabgleich hinzugefügt, die Regel dann bearbeitet und zum Rule JSON editor (JSON-Regel-Editor) gewechselt wurde. Sie können den JSON-Code für eine Regelgruppe oder Web-ACL auch über die APIs oder die Befehlszeilenschnittstelle abrufen.

Themen

- [Abgleich mit einer lokalen Bezeichnung](#)
- [Abgleich mit einer Bezeichnung aus einem anderen Kontext](#)
- [Abgleich mit einer Bezeichnung einer verwalteten Regelgruppe](#)
- [Abgleich mit einem lokalen Namespace](#)
- [Abgleich mit einem Namespace einer verwalteten Regelgruppe](#)

Abgleich mit einer lokalen Bezeichnung

Die folgende JSON-Auflistung zeigt eine Anweisung zum Abgleichen mit einer Bezeichnung, die der Webanforderung lokal hinzugefügt wurde, im gleichen Kontext wie diese Regel.

```
Rule: {
  Name: "match_rule",
  Statement: {
    LabelMatchStatement: {
      Scope: "LABEL",
```

```

        Key: "header:encoding:utf8"
    }
},
RuleLabels: [
    ...generate_more_labels...
],
Action: { Block: {} }
}

```

Wenn Sie diese Abgleichsanweisung im Konto 111122223333 in einer Regel verwenden, die Sie für Web-ACL testWebACL definieren, würde sie mit den folgenden Bezeichnungen übereinstimmen.

```
awsfaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

```
awsfaf:111122223333:webacl:testWebACL:testNS1:testNS2:header:encoding:utf8
```

Sie würde nicht auf die folgende Bezeichnung zutreffen, da die Zeichenfolge der Bezeichnung keine exakte Übereinstimmung darstellt.

```
awsfaf:111122223333:webacl:testWebACL:header:encoding2:utf8
```

Sie würde nicht mit der folgenden Bezeichnung übereinstimmen, da der Kontext nicht derselbe ist, sodass das Präfix nicht übereinstimmt. Dies gilt auch dann, wenn Sie die Regelgruppe productionRules der Web-ACL testWebACL hinzugefügt haben, in der die Regel definiert ist.

```
awsfaf:111122223333:rulegroup:productionRules:header:encoding:utf8
```

Abgleich mit einer Bezeichnung aus einem anderen Kontext

Die folgende JSON-Auflistung zeigt eine Regel für den Abgleich von Bezeichnungen, die einen Abgleich mit einer Bezeichnung aus einer Regel innerhalb einer vom Benutzer erstellten Regelgruppe durchführt. Das Präfix ist in der Spezifikation für alle Regeln erforderlich, die in der Web-ACL laufen und nicht Teil der benannten Regelgruppe sind. Diese Beispielspezifikation für eine Bezeichnung stimmt nur mit der genauen Bezeichnung überein.

```

Rule: {
  Name: "match_rule",
  Statement: {
    LabelMatchStatement: {

```



```

        Scope: "LABEL",
        Key: "awsawf:111122223333:rulegroup:testRules:header:encoding:utf8"
    }
},
RuleLabels: [
    ...generate_more_labels...
],
Action: { Block: {} }
}

```

Abgleich mit einer Bezeichnung einer verwalteten Regelgruppe

Dies ist ein Spezialfall des Abgleichs mit einer Bezeichnung, die aus einem anderen Kontext als dem der Abgleichsregel stammt. Die folgende JSON-Auflistung zeigt eine Anweisung zum Abgleich mit einer Bezeichnung für eine verwaltete Regelgruppe. Sie stimmt nur mit der exakten Bezeichnung überein, die in der Schlüsseinstellung der Abgleichsanweisung angegeben ist.

```

Rule: {
  Name: "match_rule",
  Statement: {
    LabelMatchStatement: {
      Scope: "LABEL",
      Key: "awsawf:managed:aws:managed-rule-set:header:encoding:utf8"
    }
  },
  RuleLabels: [
    ...generate_more_labels...
  ],
  Action: { Block: {} }
}

```

Abgleich mit einem lokalen Namespace

Die folgende JSON-Auflistung zeigt eine Anweisung zum Abgleich von Bezeichnungen für einen lokalen Namespace.

```

Rule: {
  Name: "match_rule",
  Statement: {
    LabelMatchStatement: {
      Scope: "NAMESPACE",
      Key: "header:encoding:"
    }
  }
}

```

```
    }
  },
  Labels: [
    ...generate_more_labels...
  ],
  Action: { Block: {} }
}
```

Ähnlich wie beim lokalen Label-Abgleich würde diese Anweisung, wenn Sie sie im Konto 111122223333 in einer Regel verwenden, die Sie für die Web-ACL testWebACL definieren, mit der folgenden Bezeichnung übereinstimmen.

```
awsmaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

Sie würde nicht mit der folgenden Bezeichnung übereinstimmen, da das Konto nicht dasselbe ist, sodass das Präfix nicht übereinstimmt.

```
awsmaf:444455556666:webacl:testWebACL:header:encoding:utf8
```

Das Präfix stimmt auch nicht mit Bezeichnungen überein, die von verwalteten Regelgruppen angewendet werden, wie die folgende.

```
awsmaf:managed:aws:managed-rule-set:header:encoding:utf8
```

Abgleich mit einem Namespace einer verwalteten Regelgruppe

Die folgende JSON-Auflistung zeigt eine Anweisung zum Abgleich mit einem Namespace für eine verwaltete Regelgruppe. Bei einer Regelgruppe, für die Sie verantwortlich sind, müssen Sie das Präfix auch für einen Namespace angeben, der außerhalb des Regelkontexts liegt.

```
Rule: {
  Name: "match_rule",
  Statement: {
    LabelMatchStatement: {
      Scope: "NAMESPACE",
      Key: "awsmaf:managed:aws:managed-rule-set:header:"
    }
  },
  RuleLabels: [
```

```
    ...generate_more_labels...  
  ],  
  Action: { Block: {} }  
}
```

Diese Spezifikation stimmt mit den folgenden Beispielbezeichnungen überein.

```
aws:waf:managed:aws:managed-rule-set:header:encoding:utf8
```

```
aws:waf:managed:aws:managed-rule-set:header:encoding:unicode
```

Sie entspricht nicht der folgenden Bezeichnung.

```
aws:waf:managed:aws:managed-rule-set:query:badstring
```

AWS WAF intelligente Bedrohungsabwehr

In diesem Abschnitt werden die verwalteten intelligenten Funktionen zur Abwehr von Bedrohungen behandelt, die von bereitgestellt werden. AWS WAF Dabei handelt es sich um fortschrittliche, spezialisierte Schutzmaßnahmen, die Sie implementieren können, um sich vor Bedrohungen wie böswilligen Bots und Kontoübernahmeversuchen zu schützen.

Note

Für die hier beschriebenen Funktionen fallen zusätzliche Kosten an, die über die Grundgebühren für die Nutzung hinausgehen. AWS WAF Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).

Die Anleitungen in diesem Abschnitt richten sich an Benutzer, die allgemein wissen, wie man AWS WAF Web-ACLs, Regeln und Regelgruppen erstellt und verwaltet. Diese Themen werden in früheren Abschnitten dieses Handbuchs behandelt.

Themen

- [Optionen für intelligente Bedrohungsabwehr](#)
- [Bewährte Methoden für intelligente Bedrohungsabwehr](#)
- [AWS WAF Webanforderungstoken](#)

- [AWS WAF Einrichtung von Konten bei der Betrugsbekämpfung und Betrugsprävention \(ACFP\)](#)
- [AWS WAF Verhinderung von Kontoübernahmen bei der Betrugsbekämpfung \(ATP\)](#)
- [AWS WAF Bot-Steuerung](#)
- [AWS WAF Integration von Client-Anwendungen](#)
- [CAPTCHA und Challenge in AWS WAF](#)

Optionen für intelligente Bedrohungsabwehr

Dieser Abschnitt bietet einen detaillierten Vergleich der Optionen für die Implementierung intelligenter Bedrohungsabwehr.

AWS WAF bietet die folgenden Schutzarten für intelligente Bedrohungsabwehr.

- AWS WAF Betrugsbekämpfung bei der Kontoerstellung und Betrugsprävention (ACFP) — Erkennt und verwaltet böswillige Versuche, Konten auf der Anmeldeseite Ihrer Anwendung einzurichten. Die Kernfunktionalität wird von der verwalteten ACFP-Regelgruppe bereitgestellt. Weitere Informationen finden Sie unter [AWS WAF Einrichtung von Konten bei der Betrugsbekämpfung und Betrugsprävention \(ACFP\)](#) und [AWS WAF Regelgruppe Betrugsprävention \(ACFP\) zur Kontoerstellung bei der Betrugsbekämpfung](#).
- AWS WAF Verhinderung von Kontoübernahmen (ATP) bei der Betrugsbekämpfung — Erkennt und verwaltet böswillige Übernahmeversuche auf der Anmeldeseite Ihrer Anwendung. Die Kernfunktionalität wird von der von ATP verwalteten Regelgruppe bereitgestellt. Weitere Informationen finden Sie unter [AWS WAF Verhinderung von Kontoübernahmen bei der Betrugsbekämpfung \(ATP\)](#) und [AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen \(ATP\) zur Betrugsbekämpfung](#).
- AWS WAF Bot-Kontrolle — Identifiziert, kennzeichnet und verwaltet sowohl freundliche als auch bösartige Bots. Diese Funktion ermöglicht die Verwaltung gängiger Bots mit anwendungsspezifischen Signaturen sowie gezielter Bots mit anwendungsspezifischen Signaturen. Die Kernfunktionalität wird von der verwalteten Regelgruppe Bot Control bereitgestellt. Weitere Informationen finden Sie unter [AWS WAF Bot-Steuerung](#) und [AWS WAF Regelgruppe „Bot-Kontrolle“](#).
- SDKs zur Integration von Client-Anwendungen — Validieren Sie Client-Sitzungen und Endbenutzer auf Ihren Webseiten und erwerben Sie AWS WAF Token, die Kunden für ihre Webanfragen verwenden können. Wenn Sie ACFP, ATP oder Bot Control verwenden, implementieren Sie die Anwendungsintegrations-SDKs nach Möglichkeit in Ihrer Client-Anwendung, um alle Funktionen der Regelgruppe optimal nutzen zu können. Wir empfehlen die Verwendung dieser Regelgruppen

ohne SDK-Integration nur als vorübergehende Maßnahme, wenn eine kritische Ressource schnell gesichert werden muss und nicht genügend Zeit für die SDK-Integration zur Verfügung steht. Informationen zur Implementierung der SDKs finden Sie unter [AWS WAF Integration von Client-Anwendungen](#).

- Challenge und CAPTCHA Regelaktionen — Validieren Sie Clientsitzungen und Endbenutzer und erwerben Sie AWS WAF Token, die Clients für ihre Webanfragen verwenden können. Sie können diese überall implementieren, wo Sie eine Regelaktion angeben, in Ihren Regeln und als Überschreibungen in Regelgruppen, die Sie verwenden. Diese Aktionen verwenden AWS WAF JavaScript Interstitials, um den Client oder Endbenutzer abzufragen, und sie erfordern Client-Anwendungen, die dies unterstützen. JavaScript Weitere Informationen finden Sie unter [CAPTCHA und Challenge in AWS WAF](#).

Die AWS verwalteten Regelgruppen ACFP, ATP und Bot Control zur intelligenten Abwehr von Bedrohungen verwenden Token für eine erweiterte Erkennung. Informationen zu den Funktionen, die Token in den Regelgruppen aktivieren, finden Sie unter [Warum sollten Sie die Anwendungsintegrations-SDKs mit ACFP verwenden](#), [Warum Sie die Anwendungsintegrations-SDKs mit ATP verwenden sollten](#), und [Warum Sie die Anwendungsintegrations-SDKs mit Bot Control verwenden sollten](#).

Ihre Optionen für die Implementierung intelligenter Bedrohungsabwehr reichen von der grundlegenden Verwendung von Regelaktionen zur Ausführung von Herausforderungen und zur Erzwingung der Token-Erfassung bis hin zu den erweiterten Funktionen, die die Regelgruppen für intelligente Bedrohungsabwehr mit AWS verwalteten Regeln bieten.

Die folgenden Tabellen bieten detaillierte Vergleiche der Optionen für die grundlegenden und erweiterten Funktionen.

Themen

- [Herausforderungen und Token-Akquisition](#)
- [Verwaltete Regelgruppen zur intelligenten Bedrohungsabwehr](#)
- [Optionen zur Ratenbegrenzung in ratenbasierten Regeln und gezielten Bot-Kontrollregeln](#)

Herausforderungen und Token-Akquisition

Mithilfe der AWS WAF Anwendungsintegrations-SDKs oder der Regelaktionen Challenge und können Sie Herausforderungen bereitstellen und Token erwerben. CAPTCHA Im Großen und

Ganzen sind die Regelaktionen einfacher zu implementieren, sie verursachen jedoch zusätzliche Kosten, beeinträchtigen Ihr Kundenerlebnis und erfordern. JavaScript Die SDKs müssen in Ihren Client-Anwendungen programmiert werden, aber sie können ein besseres Kundenerlebnis bieten, sie sind kostenlos und können mit JavaScript oder in Android- oder iOS-Anwendungen verwendet werden. Sie können die Anwendungsintegrations-SDKs nur mit Web-ACLs verwenden, die eine der kostenpflichtigen verwalteten Regelgruppen zur intelligenten Bedrohungsabwehr verwenden, die im folgenden Abschnitt beschrieben werden.

Vergleich der Optionen für Challenges und Token-Akquisition

	Challenge-Regelaktion	CAPTCHA-Regelaktion	JavaScript SDK-Herausforderung	Herausforderung für das mobile SDK
Was es ist	Regelaktion, die den Erwerb des AWS WAF Tokens erzwingt, indem sie dem Browser-Client eine stitielle Abfrage vorlegt	Regelaktion, die den Erwerb des AWS WAF Tokens erzwingt, indem der Client-Endbenutzer vor eine visuelle oder akustische Aufforderung gestellt wird	Anwendung sintegrat ionsebene für Clientbrowser und andere Geräte, die ausgeführt werden. JavaScript Rendert die stille Aufforderung und erwirbt ein Token	Anwendung sintegrat ionsebene für Android- und iOS-Anwendungen. Rendert die stille Herausforderung nativ und erwirbt ein Token
Gute Wahl für...	Automatische Validierung gegen Bot-Sitzungen und Durchsetzung des Token-Erwerbs für Kunden, die Support anbieten JavaScript	Endbenutzer- und stille Validierung gegen Bot-Sitzungen und Durchsetzung des Token-Erwerbs, für Kunden, die Folgendes	Automatische Validierung anhand von Bot-Sitzungen und Durchsetzung des Token-Erwerbs für Kunden, die Support anbieten JavaScript.	Automatische Validierung gegen Bot-Sitzungen und Durchsetzung der Token-Übernahme für native mobile Anwendungen

	Challenge-Regelaktion	CAPTCHA-Regelaktion	JavaScript SDK-Herausforderung	Herausforderung für das mobile SDK
		unterstützen JavaScript	Die SDKs bieten die niedrigste Latenz und die beste Kontrolle darüber, wo das Challenge-Skript in der Anwendung ausgeführt wird.	auf Android und iOS. Die SDKs bieten die niedrigste Latenz und die beste Kontrolle darüber, wo das Challenge-Skript in der Anwendung ausgeführt wird.
Überlegungen zur Implementierung	Als Einstellung für Regelaktionen implementiert	Als Einstellung für Regelaktionen implementiert	Erfordert eine der kostenpflichtigen ACFP-, ATP- oder Bot Control-Regelgruppen in der Web-ACL. Erfordert Codierung in der Client-Anwendung.	Erfordert eine der kostenpflichtigen ACFP-, ATP- oder Bot Control-Regelgruppen in der Web-ACL. Erfordert Codierung in der Client-Anwendung.

	Challenge-Regelaktion	CAPTCHA-Regelaktion	JavaScript SDK-Herausforderung	Herausforderung für das mobile SDK
Überlegungen zur Laufzeit	Intrusiver Ablauf für Anfragen ohne gültige Token. Der Client wird zu einem AWS WAF Challenge-Interstitial umgeleitet. Fügt Netzwerk-Roundtrips hinzu und erfordert eine zweite Auswertung der Webanfrage.	Intrusiver Flow für Anfragen ohne gültige Token. Der Client wird zu einem AWS WAF CAPTCHA-Interstitial umgeleitet. Fügt Netzwerk-Roundtrips hinzu und erfordert eine zweite Auswertung der Webanfrage.	Kann hinter den Kulissen ausgeführt werden. Gibt dir mehr Kontrolle über das Herausforderungserlebnis.	Kann hinter den Kulissen ausgeführt werden. Gibt dir mehr Kontrolle über das Herausforderungserlebnis.
Erfordert JavaScript	Ja	Ja	Ja	Nein
Unterstützte Clients	Browser und Geräte, die Javascript ausführen	Browser und Geräte, die Javascript ausführen	Browser und Geräte, die Javascript ausführen	Android- und iOS-Geräte

	Challenge-Regelaktion	CAPTCHA-Regelaktion	JavaScript SDK-Herausforderung	Herausforderung für das mobile SDK
Unterstützt einseitige Anwendungen (SPA)	Nur Durchsetzung. Sie können die Challenge Aktion in Verbindung mit den SDKs verwenden, um sicherzustellen, dass Anfragen über ein gültiges Challenge-Token verfügen. Sie können die Regelaktion nicht verwenden, um das Challenge-Skript an die Seite zu übermitteln.	Nur Durchsetzung. Sie können die CAPTCHA Aktion in Verbindung mit den SDKs verwenden, um sicherzustellen, dass Anfragen über ein gültiges CAPTCHA-Token verfügen. Sie können die Regelaktion nicht verwenden, um das CAPTCHA-Skript an die Seite zu übermitteln.	Ja	N/A

	Challenge-Regelaktion	CAPTCHA-Regelaktion	JavaScript SDK-Herausforderung	Herausforderung für das mobile SDK
Zusätzliche Kosten	Ja, für Aktionseinstellungen, die Sie explizit angeben, entweder in den Regeln, die Sie definieren, oder als Regelaktionsüberschreibungen in Regelgruppen, die Sie verwenden. Nein in allen anderen Fällen.	Ja, für Aktionseinstellungen, die Sie explizit angeben, entweder in den Regeln, die Sie definieren, oder als Regelaktionsüberschreibungen in Regelgruppen, die Sie verwenden. Nein in allen anderen Fällen.	Nein, erfordert aber eine der kostenpflichtigen Regelgruppen ACFP, ATP oder Bot Control.	Nein, erfordert aber eine der kostenpflichtigen Regelgruppen ACFP, ATP oder Bot Control.

[Einzelheiten zu den mit diesen Optionen verbundenen Kosten finden Sie in den Informationen zur intelligenten Abwehr von Bedrohungen unter AWS WAF Preise.](#)

Es kann einfacher sein, Herausforderungen auszuführen und die grundlegende Durchsetzung von Tokens zu gewährleisten, indem Sie einfach eine Regel mit einer Challenge CAPTCHA ODER-Aktion hinzufügen. Möglicherweise müssen Sie die Regelaktionen verwenden, z. B. wenn Sie keinen Zugriff auf den Anwendungscode haben.

Wenn Sie die SDKs implementieren können, können Sie jedoch Kosten sparen und die Latenz bei der Web-ACL-Auswertung von Client-Webanfragen reduzieren, verglichen mit der Challenge Aktion:

- Sie können Ihre SDK-Implementierung so schreiben, dass die Herausforderung an einem beliebigen Punkt in Ihrer Anwendung ausgeführt wird. Sie können das Token im Hintergrund abrufen, bevor ein Kunde eine Webanfrage an Ihre geschützte Ressource sendet. Auf diese Weise kann das Token zusammen mit der ersten Anfrage Ihres Kunden gesendet werden.
- Wenn Sie stattdessen Token erwerben, indem Sie eine Regel mit der Challenge Aktion implementieren, müssen die Regel und die Aktion zusätzlich ausgewertet und verarbeitet werden,

wenn der Client eine Anfrage zum ersten Mal sendet und wenn das Token abläuft. Die Challenge Aktion blockiert die Anfrage, die kein gültiges, noch nicht abgelaufenes Token hat, und sendet die Anfrage interstitial zurück an den Client. Nachdem der Client die Anfrage erfolgreich beantwortet hat, sendet das Interstitial erneut die ursprüngliche Webanforderung mit dem gültigen Token, das dann ein zweites Mal von der Web-ACL ausgewertet wird.

Verwaltete Regelgruppen zur intelligenten Bedrohungsabwehr

Die Regelgruppen für intelligente Bedrohungsabwehr (AWS Managed Rules) ermöglichen die Verwaltung grundlegender Bots, die Erkennung und Abwehr ausgeklügelter bössartiger Bots, die Erkennung und Abwehr von Kontoübernahmeversuchen sowie die Erkennung und Abwehr betrügerischer Kontoerstellungsversuche. Diese Regelgruppen bieten zusammen mit den im vorherigen Abschnitt beschriebenen SDKS für die Anwendungsintegration den fortschrittlichsten Schutz und die sicherste Kopplung mit Ihren Client-Anwendungen.

Vergleich der Gruppenoptionen für verwaltete Regeln

	ACFP	ATP	Bot Control auf gemeinsamer Ebene	Zielstufe von Bot Control
Was ist es	Verwaltet Anfragen, die Teil betrügerischer Versuche zur Kontoerstellung auf den Registrierungs- und Anmeldeseiten einer Anwendung sein könnten. Verwaltet keine Bots. Siehe AWS WAF Regelgrup	Verwaltet Anfragen, die Teil böswilliger Übernahmeversuche auf der Anmeldeseite einer Anwendung sein könnten. Verwaltet keine Bots. Siehe AWS WAF Regelgruppe zur Verhinderung von Kontoüber	Verwaltet gängige Bots, die sich selbst identifizieren, mit Signaturen, die für jede Anwendung einzigartig sind. Siehe AWS WAF Regelgruppe „Bot-Kontrolle“ .	Verwaltet gezielte Bots, die sich nicht selbst identifizieren, mit anwendungsspezifischen Signaturen. Siehe AWS WAF Regelgruppe „Bot-Kontrolle“ .

	ACFP	ATP	Bot Control auf gemeinsamer Ebene	Zielstufe von Bot Control
	<u>pe Betrugspr</u> <u>ävention (ACFP)</u> <u>zur Kontoerst</u> <u>ellung bei der</u> <u>Betrugsbe</u> <u>kämpfung.</u>	<u>nahmen (ATP)</u> <u>zur Betrugsbe</u> <u>kämpfung.</u>		

	ACFP	ATP	Bot Control auf gemeinsamer Ebene	Zielstufe von Bot Control
Gute Wahl für...	Überprüfung des Datenverkehrs bei der Kontoerstellung auf betrügerische Angriffe zur Kontoerstellung, z. B. auf Versuche bei der Erstellung von Benutzernamen und viele neue Konten, die von einer einzigen IP-Adresse aus erstellt wurden.	Überprüfung des Anmeldeverkehrs auf Angriffe zur Kontoübernahme, wie z. B. Anmeldeversuche mit Passwortschreibung und viele Anmeldeversuche von derselben IP-Adresse aus. Bei Verwendung mit Tokens bietet sie außerdem umfassende Schutzmaßnahmen wie die Begrenzung der Geschwindigkeit von IP-Adressen und Client-Sitzungen für eine große Anzahl fehlgeschlagener Anmeldeversuche.	Grundlegender Bot-Schutz und Kennzeichnung von allgemeinem, automatisiertem Bot-Traffic.	Gezielter Schutz vor ausgeklügelten Bots, einschließlich Ratenbegrenzung auf der Ebene der Clientsitzung und Erkennung und Abwehr von Browser-Automatisierungstools wie Selenium und Puppeteer.

	ACFP	ATP	Bot Control auf gemeinsamer Ebene	Zielstufe von Bot Control
Fügt Beschriftungen hinzu, die auf Bewertungsergebnisse hinweisen	Ja	Ja	Ja	Ja
Fügt Token-Labels hinzu	Ja	Ja	Ja	Ja
Blockierung für Anfragen, die kein gültiges Token haben	Nicht enthalten. Siehe Anfragen blockieren, die kein gültiges Token haben.	Nicht enthalten. Siehe Anfragen blockieren, die kein gültiges Token haben.	Nicht enthalten. Siehe Anfragen blockieren, die kein gültiges Token haben.	Blockiert Clientsitzungen, die 5 Anfragen ohne Token senden.
Erfordert das AWS WAF Token <code>aws-waf-token</code>	Für alle Regeln erforderlich. Siehe Warum sollten Sie die Anwendung integrations-SDKs mit ACFP verwenden.	Für viele Regeln erforderlich. Siehe Warum Sie die Anwendung integrations-SDKs mit ATP verwenden sollten.	Nein	Ja

	ACFP	ATP	Bot Control auf gemeinsamer Ebene	Zielstufe von Bot Control
Erwirbt das AWS WAF Token <code>aws-waf-token</code>	Ja, durch die Regel <code>AllRequests</code> erzwungen	Nein	Nein	Manche Regeln verwenden Challenge oder CAPTCHA regeln Aktionen, bei denen Tokens erworben werden.

Einzelheiten zu den mit diesen Optionen verbundenen Kosten finden Sie in den Informationen zur intelligenten Abwehr von Bedrohungen unter [AWS WAF Preise](#).

Optionen zur Ratenbegrenzung in ratenbasierten Regeln und gezielten Bot-Kontrollregeln

Sowohl die Zielstufe der AWS WAF Bot-Control-Regelgruppe als auch die AWS WAF ratenbasierte Regelaussage ermöglichen eine Begrenzung der Rate von Webanfragen. In der folgenden Tabelle werden die beiden Optionen verglichen.

Vergleich der Optionen für ratenbasierte Erkennung und Schadensbegrenzung

	AWS WAF ratenbasierte Regel	AWS WAF Gezielte Regeln von Bot Control
Wie wird die Ratenbegrenzung angewendet	Geht auf Gruppen von Anfragen ein, die zu häufig eingehen. Sie können jede Aktion anwenden, mit Ausnahme von <code>Allow</code> .	Erzwingt menschenähnliche Zugriffsmuster und wendet mithilfe von Anforderungstoken eine dynamische Ratenbegrenzung an.

	AWS WAF ratenbasierte Regel	AWS WAF Gezielte Regeln von Bot Control	
Basierend auf historischen Verkehrsdaten?	Nein	Ja	
Zeit, die benötigt wird, um historische Verkehrsbasislinien zu sammeln	N/A	Fünf Minuten für dynamische Schwellenwerte. N/A für fehlendes Token.	
Verzögerung bei der Schadensbegrenzung	Normalerweise 30-50 Sekunden. Kann bis zu mehreren Minuten dauern.	Normalerweise weniger als 10 Sekunden. Kann bis zu mehreren Minuten dauern.	
Minderungsziele	Konfigurierbar. Sie können Anfragen mithilfe einer Scope-Down-Anweisung und nach einem oder mehreren Aggregationschlüsseln wie IP-Adresse, HTTP-Methode und Abfragezeichenfolge gruppieren.	IP-Adressen und Clientsitzungen	
Um Abhilfemaßnahmen auszulösen, ist das Verkehrsvolumen erforderlich	Mittel — im angegebenen Zeitfenster können es nur 100 Anfragen sein	Niedrig — dient zur Erkennung von Client-Mustern wie langsamen Scrapern	
Individuell anpassbare Schwellenwerte	Ja	Nein	

	AWS WAF ratenbasierte Regel	AWS WAF Gezielte Regeln von Bot Control	
Standardmäßige Abhilfemaßnahmen	<p>Die Standardinstellung für die Konsole ist Block. Keine Standardinstellung in der API; die Einstellung ist erforderlich.</p> <p>Sie können dies auf jede beliebige Regelaktion festlegen, mit Ausnahme von Allow.</p>	<p>Die Einstellungen für Regelgruppenregelaktionen gelten Challenge für fehlende Token und CAPTCHA für hohen Datenverkehr aus einer einzelnen Clientsitzung.</p> <p>Sie können jede dieser Regeln auf eine beliebige gültige Regelaktion festlegen.</p>	
Widerstandsfähigkeit gegen stark verteilte Angriffe	Mittel — maximal 10.000 IP-Adressen für eine alleinige IP-Adressbegrenzung	Mittel — zwischen IP-Adressen und Tokens auf insgesamt 50.000 begrenzt	
AWS WAF Preise	In den Standardgebühren für enthaltenes AWS WAF.	In den Gebühren für die angestrebte Stufe der intelligenten Bedrohungssabwehr mit Bot Control enthalten.	
Für weitere Informationen	Ratenbasierte Regelanweisung	AWS WAF Regelgruppe „Bot-Kontrolle“	

Bewährte Methoden für intelligente Bedrohungsabwehr

Folgen Sie den bewährten Methoden in diesem Abschnitt, um die Funktionen zur intelligenten Bedrohungsabwehr am effizientesten und kostengünstigsten zu implementieren.

- Implementieren Sie die SDKs JavaScript und die Integration mobiler Anwendungen — Implementieren Sie die Anwendungsintegration, um den vollen Funktionsumfang von ACFP, ATP oder Bot Control so effektiv wie möglich zu nutzen. Die verwalteten Regelgruppen verwenden die von den SDKs bereitgestellten Token, um legitimen Client-Verkehr auf Sitzungsebene von unerwünschtem Datenverkehr zu trennen. Die SDKs für die Anwendungsintegration stellen sicher, dass diese Token immer verfügbar sind. Details dazu finden Sie unter:
 - [Warum sollten Sie die Anwendungsintegrations-SDKs mit ACFP verwenden](#)
 - [Warum Sie die Anwendungsintegrations-SDKs mit ATP verwenden sollten](#)
 - [Warum Sie die Anwendungsintegrations-SDKs mit Bot Control verwenden sollten](#)

Verwenden Sie die Integrationen, um Herausforderungen in Ihrem Client zu implementieren und beispielsweise die Art und Weise anzupassen JavaScript, wie CAPTCHA-Rätsel Ihren Endbenutzern präsentiert werden. Details hierzu finden Sie unter [AWS WAF Integration von Client-Anwendungen](#).

Wenn Sie CAPTCHA-Rätsel mithilfe der JavaScript API anpassen und die CAPTCHA Regelaktion an einer beliebigen Stelle in Ihrer Web-ACL verwenden, folgen Sie den Anweisungen für den Umgang mit der AWS WAF CAPTCHA-Antwort in Ihrem Client unter [Umgang mit einer CAPTCHA-Antwort von AWS WAF](#). Diese Anleitung gilt für alle Regeln, die die CAPTCHA Aktion verwenden, einschließlich der Regeln in der verwalteten ACFP-Regelgruppe und der angestrebten Schutzstufe der verwalteten Regelgruppe Bot Control.

- Beschränken Sie die Anfragen, die Sie an die Regelgruppen ACFP, ATP und Bot Control senden. Für die Nutzung der Regelgruppen mit intelligenten AWS verwalteten Regeln zur Abwehr von Bedrohungen fallen zusätzliche Gebühren an. Die ACFP-Regelgruppe überprüft Anfragen an die von Ihnen angegebenen Endpunkte für die Kontoregistrierung und Kontoerstellung. Die ATP-Regelgruppe überprüft Anfragen an den von Ihnen angegebenen Anmeldeendpunkt. Die Bot Control-Regelgruppe überprüft jede Anfrage, die sie bei der Web-ACL-Bewertung erreicht.

Ziehen Sie die folgenden Ansätze in Betracht, um die Verwendung dieser Regelgruppen zu reduzieren:

- Schließen Sie Anfragen von der Prüfung aus, wenn Sie in der Erklärung zur verwalteten Regelgruppe eine Erklärung zum Umfang angeben. Sie können dies mit jeder verschachtelten Anweisung tun. Weitere Informationen finden Sie unter [Eingrenzungsanweisungen](#).
- Schließen Sie Anfragen von der Prüfung aus, indem Sie Regeln vor der Regelgruppe hinzufügen. Für Regeln, die Sie nicht in einer Scope-down-Anweisung verwenden können, und für komplexere Situationen, wie z. B. die Kennzeichnung gefolgt von der Zuordnung von Bezeichnungen, möchten Sie möglicherweise Regeln hinzufügen, die vor den Regelgruppen ausgeführt werden. Weitere Informationen finden Sie unter [Eingrenzungsanweisungen](#) und [Grundlagen der Regelerklärung](#).
- Führen Sie die Regelgruppen nach kostengünstigeren Regeln aus. Wenn Sie andere AWS WAF Standardregeln haben, die Anfragen aus irgendeinem Grund blockieren, führen Sie sie vor diesen kostenpflichtigen Regelgruppen aus. Weitere Informationen zu Regeln und Regelverwaltung finden Sie unter [Grundlagen der Regelerklärung](#).
- Wenn Sie mehr als eine der Regelgruppen mit intelligenter Bedrohungsabwehr verwenden, führen Sie sie aus Kostengründen in der folgenden Reihenfolge aus: Bot Control, ATP, ACFP.

Weitere Informationen finden Sie unter [AWS WAF -Preise](#).

- Aktivieren Sie die gezielte Schutzstufe der Regelgruppe Bot Control bei normalem Web-Verkehr — Einige Regeln der Zielschutzstufe benötigen Zeit, um Basiswerte für normale Datenverkehrsmuster festzulegen, bevor sie unregelmäßige oder bösartige Datenverkehrsmuster erkennen und darauf reagieren können. Beispielsweise benötigen die TGT_ML_* Regeln bis zu 24 Stunden, um sich aufzuwärmen.

Fügen Sie diese Schutzmaßnahmen hinzu, wenn Sie nicht von einem Angriff betroffen sind, und geben Sie ihnen Zeit, ihre Grundlinien festzulegen, bevor sie erwarten, dass sie angemessen auf Angriffe reagieren. Wenn Sie diese Regeln während eines Angriffs hinzufügen, nachdem der Angriff abgeklungen ist, dauert die Erstellung einer Basislinie normalerweise doppelt bis dreimal so lange wie normalerweise erforderlich, da der Angriffsverkehr zu Verzerrungen führt. Weitere Informationen zu den Regeln und den dafür erforderlichen Aufwärmzeiten finden Sie unter [Liste der Regeln](#)

- Verwenden Sie für den Schutz vor Distributed-Denial-of-Service (DDoS) Shield Advanced die automatische DDoS-Abwehr auf Anwendungsebene. Die Regelgruppen zur intelligenten Bedrohungsabwehr bieten keinen DDoS-Schutz. ACFP schützt vor betrügerischen Versuchen, auf der Anmeldeseite Ihrer Anwendung ein Konto zu erstellen. ATP schützt vor Kontoübernahmeversuchen auf Ihrer Anmeldeseite. Bot Control konzentriert sich auf die

Durchsetzung menschenähnlicher Zugriffsmuster mithilfe von Tokens und dynamischer Ratenbegrenzung bei Clientsitzungen.

Wenn Sie Shield Advanced mit aktivierter automatischer DDoS-Abwehr auf Anwendungsebene verwenden, reagiert Shield Advanced automatisch auf erkannte DDoS-Angriffe, indem es in Ihrem Namen benutzerdefinierte AWS WAF Abwehr erstellt, bewertet und einsetzt. Weitere Informationen zu Shield Advanced finden Sie [AWS Shield Advanced Überblick](#) unter und [AWS Shield Advanced Schutzmaßnahmen auf Anwendungsebene \(Schicht 7\)](#).

- Feinabstimmung und Konfiguration der Token-Behandlung — Passen Sie die Token-Behandlung der Web-ACL an, um eine optimale Benutzererfahrung zu erzielen.
 - Um die Betriebskosten zu senken und das Nutzererlebnis zu verbessern, sollten Sie die Immunitätszeiten Ihrer Tokenverwaltung so lange einstellen, wie es Ihre Sicherheitsanforderungen zulassen. Dadurch wird der Einsatz von CAPTCHA-Rätseln und stillen Herausforderungen auf ein Minimum reduziert. Weitere Informationen finden Sie unter [Ablauf des Zeitstempels: Zeiten der Token-Immunität](#).
 - Um die gemeinsame Nutzung von Token zwischen geschützten Anwendungen zu ermöglichen, konfigurieren Sie eine Token-Domainliste für Ihre Web-ACL. Weitere Informationen finden Sie unter [Token-Domains und Domainlisten](#).
- Anfragen mit beliebigen Hostspezifikationen ablehnen — Konfigurieren Sie Ihre geschützten Ressourcen so, dass die Host Header in Webanfragen mit der Zielressource übereinstimmen müssen. Sie können einen Wert oder eine bestimmte Gruppe von Werten akzeptieren, z. B. `myExampleHost.com` und `www.myExampleHost.com`, aber Sie können keine beliebigen Werte für den Host akzeptieren.
- Für Application Load Balancer, die Ursprünge für CloudFront Distributionen sind, konfigurieren CloudFront und AWS WAF für die korrekte Token-Behandlung sorgen — Wenn Sie Ihre Web-ACL einem Application Load Balancer zuordnen und den Application Load Balancer als Ursprung für eine CloudFront Distribution bereitstellen, finden Sie weitere Informationen unter [Konfiguration erforderlich für Application Load Balancer, die Origins sind CloudFront](#)
- Testen und Optimieren vor der Bereitstellung — Bevor Sie Änderungen an Ihrer Web-ACL vornehmen, sollten Sie die Test- und Optimierungsverfahren in diesem Handbuch befolgen, um sicherzustellen, dass Sie das erwartete Verhalten erhalten. Dies ist besonders wichtig für diese kostenpflichtigen Funktionen. Allgemeine Hinweise finden Sie unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#). Spezifische Informationen zu den kostenpflichtigen verwalteten Regelgruppen finden Sie unter [Testen und Bereitstellen von ACFPTesten und Bereitstellen von ATP](#), und [Testen und Bereitstellen von AWS WAF Bot Control](#).

AWS WAF Webanforderungstoken

AWS WAF Tokens sind ein integraler Bestandteil des verbesserten Schutzes, den AWS WAF intelligente Bedrohungsabwehr bietet. Ein Token, manchmal auch Fingerabdruck genannt, ist eine Sammlung von Informationen über eine einzelne Clientsitzung, die der Client speichert und bei jeder Webanfrage bereitstellt. AWS WAF verwendet Token, um böswillige Clientsitzungen zu identifizieren und von legitimen Sitzungen zu trennen, selbst wenn beide von einer einzigen IP-Adresse stammen. Die Verwendung von Token verursacht Kosten, die für legitime Benutzer vernachlässigbar, für Botnets jedoch in großem Umfang teuer sind.

AWS WAF verwendet Tokens zur Unterstützung seiner Browser- und Endbenutzer-Challenge-Funktionalität, die von den Anwendungsintegrations-SDKs und den Regelaktionen und bereitgestellt wird. Challenge CAPTCHA Darüber hinaus ermöglichen Tokens Funktionen der verwalteten Regelgruppen AWS WAF Bot-Kontrolle und Verhinderung von Kontoübernahmen.

AWS WAF erstellt, aktualisiert und verschlüsselt Token für Kunden, die erfolgreich auf stille Herausforderungen und CAPTCHA-Rätsel reagieren. Wenn ein Client mit einem Token eine Webanforderung sendet, schließt er das verschlüsselte Token ein, AWS WAF entschlüsselt das Token und verifiziert seinen Inhalt.

Themen

- [Wie AWS WAF verwendet Tokens](#)
- [Token-Eigenschaften](#)
- [Ablauf des Zeitstempels: Zeiten der Token-Immunität](#)
- [Token-Domains und Domainlisten](#)
- [Token-Kennzeichnung durch die verwalteten Regelgruppen zur intelligenten Bedrohungsabwehr](#)
- [Anfragen blockieren, die kein gültiges Token haben](#)
- [Konfiguration erforderlich für Application Load Balancer, die Origins sind CloudFront](#)

Wie AWS WAF verwendet Tokens

AWS WAF verwendet Token, um die folgenden Arten der Validierung von Clientsitzungen aufzuzeichnen und zu überprüfen:

- CAPTCHA — CAPTCHA-Rätsel helfen dabei, Bots von menschlichen Benutzern zu unterscheiden. Ein CAPTCHA wird nur durch die Regelaktion ausgeführt. CAPTCHA Nach erfolgreicher Lösung

des Rätsels aktualisiert das CAPTCHA-Skript den CAPTCHA-Zeitstempel des Tokens. Weitere Informationen finden Sie unter [CAPTCHA und Challenge in AWS WAF](#).

- Herausforderung — Herausforderungen werden im Hintergrund ausgeführt, um reguläre Kundensitzungen von Bot-Sitzungen zu unterscheiden und den Betrieb für Bots teurer zu machen. Wenn die Herausforderung erfolgreich abgeschlossen wurde, ruft das Challenge-Skript bei AWS WAF Bedarf automatisch ein neues Token ab und aktualisiert dann den Challenge-Zeitstempel des Tokens.

AWS WAF führt Herausforderungen in den folgenden Situationen aus:

- Anwendungsintegrations-SDKs — Die Anwendungsintegrations-SDKs werden in Ihren Client-Anwendungssitzungen ausgeführt und stellen sicher, dass Anmeldeversuche nur zulässig sind, nachdem der Client erfolgreich auf eine Anfrage reagiert hat. Weitere Informationen finden Sie unter [AWS WAF Integration von Client-Anwendungen](#).
- ChallengeRegelaktion — Weitere Informationen finden Sie unter [CAPTCHA und Challenge in AWS WAF](#).
- CAPTCHA— Wenn ein CAPTCHA-Interstitial ausgeführt wird und der Client noch kein Token hat, führt das Skript automatisch zuerst eine Abfrage aus, um die Clientsitzung zu verifizieren und das Token zu initialisieren.

Tokens sind für viele Regeln in den Regelgruppen „Intelligent Threat AWS Managed Rules“ erforderlich. Die Regeln verwenden Token, um beispielsweise zwischen Clients auf Sitzungsebene zu unterscheiden, Browsereigenschaften zu bestimmen und den Grad der menschlichen Interaktivität auf der Anwendungswebseite zu verstehen. Diese Regelgruppen rufen die AWS WAF Tokenverwaltung auf, bei der Token-Labels angewendet werden, die dann von den Regelgruppen überprüft werden.

- AWS WAF Betrugskontrolle, Kontoerstellung, Betrugsprävention (ACFP) — Die ACFP-Regeln erfordern Webanfragen mit gültigen Tokens. Weitere Informationen zu den Regeln finden Sie unter [AWS WAF Regelgruppe Betrugsprävention \(ACFP\) zur Kontoerstellung bei der Betrugsbekämpfung](#).
- AWS WAF Verhinderung von Kontoübernahmen (ATP) bei der Betrugsbekämpfung — Die ATP-Regeln zur Verhinderung umfangreicher und lang andauernder Kundensitzungen erfordern Webanfragen, die ein gültiges Token mit einem noch nicht abgelaufenen Challenge-Zeitstempel enthalten. Weitere Informationen finden Sie unter [AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen \(ATP\) zur Betrugsbekämpfung](#).

- **AWS WAF Bot-Kontrolle** — Die gezielten Regeln in dieser Regelgruppe begrenzen die Anzahl der Webanfragen, die ein Client ohne gültiges Token senden kann, und sie verwenden die Token-Sitzungsverfolgung für die Überwachung und Verwaltung auf Sitzungsebene. Je nach Bedarf wenden die Regeln die Aktionen an Challenge und CAPTCHA regeln die Aktionen, um die Token-Erfassung und ein gültiges Kundenverhalten durchzusetzen. Weitere Informationen finden Sie unter [AWS WAF Regelgruppe „Bot-Kontrolle“](#).

Token-Eigenschaften

Jedes Token hat die folgenden Eigenschaften:

- Das Token wird in einem Cookie mit dem Namen gespeichert `aws-waf-token`.
- Das Token ist verschlüsselt.
- Das Token gibt der Clientsitzung einen Fingerabdruck mit einem festen, detaillierten Bezeichner, der die folgenden Informationen enthält:
 - Der Zeitstempel der letzten erfolgreichen Antwort des Clients auf eine unbeaufsichtigte Aufforderung.
 - Der Zeitstempel der letzten erfolgreichen Antwort des Endbenutzers auf ein CAPTCHA. Dies ist nur vorhanden, wenn Sie CAPTCHA in Ihren Schutzmaßnahmen verwenden.
 - Zusätzliche Informationen über den Kunden und das Verhalten des Kunden, die dazu beitragen können, Ihre legitimen Kunden vor unerwünschtem Datenverkehr zu schützen. Zu den Informationen gehören verschiedene Kundenkennungen und clientseitige Signale, die zur Erkennung automatisierter Aktivitäten verwendet werden können. Die gesammelten Informationen sind nicht eindeutig und können nicht einer einzelnen Person zugeordnet werden.
 - Alle Token enthalten Daten aus der Abfrage des Client-Browsers, z. B. Hinweise auf Automatisierung und Inkonsistenzen bei den Browsereinstellungen. Diese Informationen werden von den Skripten abgerufen, die von der Challenge Aktion ausgeführt werden, und von den SDKs der Client-Anwendung. Die Skripts fragen den Browser aktiv ab und fügen die Ergebnisse in das Token ein.
 - Wenn Sie ein SDK für die Integration von Client-Anwendungen implementieren, enthält das Token außerdem passiv gesammelte Informationen über die Interaktivität des Endbenutzers mit der Anwendungsseite. Interaktivität umfasst Mausbewegungen, Tastendrucke und Interaktionen mit beliebigen HTML-Formularen, die auf der Seite vorhanden sind. Diese Informationen helfen dabei, den Grad der menschlichen Interaktivität im Client zu AWS WAF

ermitteln, um Benutzer herauszufordern, die keine Menschen zu sein scheinen. Hinweise zu clientseitigen Integrationen finden Sie unter [AWS WAF Integration von Client-Anwendungen](#)

Bietet aus Sicherheitsgründen AWS keine vollständige Beschreibung des AWS WAF Tokeninhalts oder detaillierte Informationen zum Token-Verschlüsselungsprozess.

Ablauf des Zeitstempels: Zeiten der Token-Immunität

AWS WAF verwendet Challenge- und CAPTCHA-Immunitätszeiten, um zu steuern, wie oft eine einzelne Clientsitzung mit einer Challenge oder einem CAPTCHA konfrontiert werden kann. Nachdem ein Endbenutzer erfolgreich auf ein CAPTCHA geantwortet hat, bestimmt die CAPTCHA-Immunitätszeit, wie lange der Endbenutzer davor gefeit ist, einem weiteren CAPTCHA präsentiert zu werden. In ähnlicher Weise bestimmt die Challenge-Immunitätszeit, wie lange eine Kundensitzung davor gefeit ist, erneut herausgefordert zu werden, nachdem sie erfolgreich auf eine Aufforderung reagiert hat.

AWS WAF zeichnet eine erfolgreiche Antwort auf eine Aufforderung oder ein CAPTCHA auf, indem der entsprechende Zeitstempel im Token aktualisiert wird. Wenn das Token auf Challenge oder CAPTCHA AWS WAF überprüft wird, subtrahiert es den Zeitstempel von der aktuellen Uhrzeit. Wenn das Ergebnis länger als die konfigurierte Immunitätszeit ist, ist der Zeitstempel abgelaufen.

Sie können die Challenge- und CAPTCHA-Immunitätszeiten in der Web-ACL und auch in jeder Regel, die die Regelaktion CAPTCHA oder Challenge verwendet, konfigurieren.

- Die Standardeinstellung der Web-ACL für beide Immunitätszeiten beträgt 300 Sekunden.
- Sie können die Immunitätszeit für jede Regel angeben, die die Challenge Aktion CAPTCHA oder verwendet. Wenn Sie die Immunitätszeit für die Regel nicht angeben, erbt sie die Einstellung von der Web-ACL.
- Wenn Sie für eine Regel innerhalb einer Regelgruppe, die die Challenge Aktion CAPTCHA oder verwendet, die Immunitätszeit für die Regel nicht angeben, erbt sie die Einstellung von jeder Web-ACL, in der Sie die Regelgruppe verwenden.
- Die Anwendungsintegrations-SDKs verwenden die Challenge-Immunitätszeit der Web-ACL.

Der Mindestwert für die Challenge-Immunitätszeit beträgt 300 Sekunden. Der Mindestwert für die CAPTCHA-Immunitätszeit beträgt 60 Sekunden. Der Höchstwert für beide Immunitätszeiten beträgt 259.200 Sekunden oder drei Tage.

Sie können die Einstellungen für die Web-ACL und die Immunitätszeit auf Regelebene verwenden, Challenge um die CAPTCHA Aktion oder das SDK-Challenge-Management-Verhalten zu optimieren. Sie können beispielsweise Regeln konfigurieren, die den Zugriff auf hochsensible Daten mit niedrigen Immunitätszeiten kontrollieren, und dann in Ihrer Web-ACL höhere Immunitätszeiten für Ihre anderen Regeln und SDKs festlegen.

Insbesondere bei CAPTCHA kann die Lösung eines Rätsels das Website-Erlebnis Ihrer Kunden verschlechtern. Wenn Sie also die CAPTCHA-Immunitätszeit anpassen, können Sie die Auswirkungen auf das Kundenerlebnis mindern und gleichzeitig den gewünschten Schutz bieten.

Weitere Informationen zur Einstellung der Immunitätszeiten für Ihre Verwendung der Aktionen und der Regel finden Sie unter [Challenge CAPTCHA Bewährte Methoden für die Verwendung der Challenge Aktionen CAPTCHA und](#)

Einstellung der Token-Immunitätszeiten

Sie können die Immunitätszeiten in Ihrer Web-ACL und in Ihren Regeln festlegen, die die Aktionen Challenge und CAPTCHA Regeln verwenden.

Allgemeine Informationen zur Verwaltung einer Web-ACL und ihrer Regeln finden Sie unter [Arbeiten mit Web-ACLs](#).

Wo wird die Immunitätszeit für eine Web-ACL festgelegt

- **Konsole** — Wenn Sie die Web-ACL bearbeiten, bearbeiten und ändern Sie auf der Registerkarte Regeln die Einstellungen in den Bereichen Web ACL CAPTCHA-Konfiguration und Web ACL Challenge. In der Konsole können Sie das Web-ACL-CAPTCHA konfigurieren und Immunitätszeiten erst dann abfragen, nachdem Sie die Web-ACL erstellt haben.
- **Außerhalb der Konsole** — Der Web-ACL-Datentyp verfügt über CAPTCHA- und Challenge-Konfigurationsparameter, die Sie konfigurieren und für Ihre Erstellungs- und Aktualisierungsvorgänge auf der Web-ACL bereitstellen können.

Wo wird die Immunitätszeit für eine Regel festgelegt

- **Konsole** — Wenn Sie eine Regel erstellen oder bearbeiten und die Challenge Aktion CAPTCHA oder angeben, können Sie die Einstellung für die Immunitätszeit der Regel ändern.
- **Außerhalb der Konsole** — Der Regeldatentyp verfügt über CAPTCHA- und Challenge-Konfigurationsparameter, die Sie bei der Definition der Regel konfigurieren können.

Token-Domains und Domainlisten

Wenn ein Token für einen Client AWS WAF erstellt wird, wird es mit einer Tokendomäne konfiguriert. Wenn AWS WAF ein Token in einer Webanforderung geprüft wird, lehnt es das Token als ungültig ab, wenn seine Domain mit keiner der Domänen übereinstimmt, die für die Web-ACL als gültig angesehen werden.

Standardmäßig werden AWS WAF nur Token akzeptiert, deren Domäneneinstellung genau mit der Hostdomäne der Ressource übereinstimmt, die der Web-ACL zugeordnet ist. Dies ist der Wert des Host Headers in der Webanforderung. In einem Browser finden Sie diese Domain in der JavaScript `window.location.hostname` Eigenschaft und in der Adresse, die Ihr Benutzer in seiner Adressleiste sieht.

Sie können auch akzeptable Token-Domänen in Ihrer Web-ACL-Konfiguration angeben, wie im folgenden Abschnitt beschrieben. In diesem Fall AWS WAF akzeptiert sowohl exakte Übereinstimmungen mit dem Host-Header als auch Übereinstimmungen mit Domänen in der Token-Domainliste.

Sie können Token-Domänen angeben AWS WAF , die bei der Festlegung der Domain und bei der Auswertung eines Tokens in einer Web-ACL verwendet werden sollen. Bei den Domänen, die Sie angeben, darf es sich nicht um öffentliche Suffixe handeln, wie z. `gov.au`. Die Domains, die Sie nicht verwenden können, finden Sie in der Liste https://publicsuffix.org/list/public_suffix_list.dat unter Liste der [öffentlichen Suffixe](#).

Konfiguration der Domainliste für Web-ACL-Tokens

Sie können eine Web-ACL so konfigurieren, dass sie Token für mehrere geschützte Ressourcen gemeinsam nutzt, indem Sie eine Token-Domainliste mit den zusätzlichen Domänen bereitstellen, die Sie akzeptieren AWS WAF möchten. Nimmt bei einer Token-Domainliste AWS WAF trotzdem die Host-Domain der Ressource an. Darüber hinaus akzeptiert sie alle Domänen in der Token-Domainliste, einschließlich ihrer Subdomänen mit Präfix.

Eine Domainspezifikation `example.com` in Ihrer Token-Domainliste entspricht beispielsweise `example.com` (von `http://example.com/`) `api.example.com`, (von `http://api.example.com/`) und `www.example.com` (von `http://www.example.com/`). Sie entspricht `example.api.com` nicht (von `http://example.api.com/`) oder `apiexample.com` (von `http://apiexample.com/`).

Sie können die Token-Domainliste in Ihrer Web-ACL konfigurieren, wenn Sie sie erstellen oder bearbeiten. Allgemeine Informationen zur Verwaltung einer Web-ACL finden Sie unter [Arbeiten mit Web-ACLs](#).

Steuern der Domäneneinstellung innerhalb des Tokens

AWS WAF erstellt Token auf Anforderung der Challenge-Skripte, die von den Anwendungsintegrations-SDKs Challenge und den CAPTCHA Regelaktionen ausgeführt werden.

Die Domäne, die ein Token AWS WAF eingibt, wird durch den Typ des Challenge-Skripts bestimmt, das es anfordert, und durch jede zusätzliche Token-Domänenkonfiguration, die Sie angeben. AWS WAF setzt die Domain im Token auf die kürzeste, allgemeinste Einstellung, die sie in der Konfiguration finden kann.

- JavaScript SDK — Sie können das JavaScript SDK mit einer Token-Domainspezifikation konfigurieren, die eine oder mehrere Domänen umfassen kann. Bei den Domänen, die Sie konfigurieren, muss es sich um Domänen handeln, AWS WAF die auf der geschützten Hostdomäne und der Tokendomänenliste der Web-ACL basieren, die akzeptiert werden.

Wenn ein AWS WAF Token für den Client ausgestellt wird, wird die Tokendomäne auf eine Domäne gesetzt, die der Hostdomäne entspricht und die kürzeste ist, sowohl aus der Hostdomäne als auch aus den Domänen in Ihrer konfigurierten Liste. Wenn die Hostdomäne beispielsweise ist `api.example.com` und die Token-Domainliste dies `hatexample.com`, AWS WAF verwendet `example.com` das Token, weil es mit der Host-Domain übereinstimmt und kürzer ist. Wenn Sie in der JavaScript API-Konfiguration keine Token-Domainliste angeben, AWS WAF wird die Domain auf die Hostdomäne der geschützten Ressource gesetzt.

Weitere Informationen finden Sie unter [Bereitstellung von Domains zur Verwendung in den Tokens](#).

- Mobiles SDK — In Ihrem Anwendungscode müssen Sie das mobile SDK mit einer Token-Domäneneigenschaft konfigurieren. Bei dieser Eigenschaft muss es sich um eine Domain handeln, AWS WAF die auf der geschützten Host-Domain und der Token-Domainliste der Web-ACL basiert, die Akzeptanz akzeptiert.

Wenn AWS WAF ein Token für den Client ausgegeben wird, verwendet er diese Eigenschaft als Tokendomäne. AWS WAF verwendet die Hostdomäne nicht in den Tokens, die es für den mobilen SDK-Client ausgibt.

Weitere Informationen finden Sie in der WAFConfiguration `domainName` Einstellung unter [Die AWS WAF mobile SDK-Spezifikation](#).

- **ChallengeAktion** — Wenn Sie in der Web-ACL eine Token-Domainliste angeben, wird die Token-Domain auf eine Domain AWS WAF gesetzt, die der Hostdomäne entspricht und die kürzeste ist, sowohl aus der Hostdomäne als auch aus den Domains in der Liste. Wenn zum Beispiel die Host-Domain `api.example.com` und die Token-Domainliste `hatexample.com`, AWS WAF verwendet `example.com` das Token, weil es mit der Host-Domain übereinstimmt und kürzer ist. Wenn Sie in der Web-ACL keine Token-Domainliste angeben, AWS WAF wird die Domain auf die Hostdomäne der geschützten Ressource gesetzt.

Token-Kennzeichnung durch die verwalteten Regelgruppen zur intelligenten Bedrohungsabwehr

In diesem Abschnitt werden die Labels beschrieben, die die AWS WAF Tokenverwaltung Webanfragen hinzufügt. Weitere Informationen zu Bezeichnungen finden Sie unter [AWS WAF Labels auf Webanfragen](#).

Wenn Sie eine der von AWS WAF Bot oder Fraud Control verwalteten Regelgruppen verwenden, verwenden die Regelgruppen die AWS WAF Tokenverwaltung, um die Webanforderungstoken zu überprüfen und die Anfragen mit Token-Labels zu versehen. Informationen zu den verwalteten Regelgruppen finden Sie unter [AWS WAF Regelgruppe Betrugsprävention \(ACFP\) zur Kontoerstellung bei der Betrugsbekämpfung](#), [AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen \(ATP\) zur Betrugsbekämpfung](#), und [AWS WAF Regelgruppe „Bot-Kontrolle“](#).


Note

AWS WAF wendet Token-Labels nur an, wenn Sie eine dieser verwalteten Regelgruppen zur intelligenten Bedrohungsabwehr verwenden.

Die Tokenverwaltung kann Webanfragen die folgenden Bezeichnungen hinzufügen.

Bezeichnung der Clientsitzung

Das Label `awsواف:managed:token:id:identifizier` enthält eine eindeutige Kennung, anhand derer die AWS WAF Tokenverwaltung die Clientsitzung identifiziert. Die Kennung kann sich ändern, wenn der Client ein neues Token erwirbt, beispielsweise nachdem er das Token, das er verwendet hat, verworfen hat.

 Note

AWS WAF meldet keine CloudWatch Amazon-Metriken für dieses Label.

Token-Statusbezeichnungen: Namespace-Präfixe für Labels

Token-Statusbezeichnungen berichten über den Status des Tokens und der darin enthaltenen Challenge- und CAPTCHA-Informationen.

Jedes Token-Statuslabel beginnt mit einem der folgenden Namespace-Präfixe:

- `awsaf:managed:token:`— Wird verwendet, um den allgemeinen Status des Tokens und den Status der Challenge-Informationen des Tokens zu melden.
- `awsaf:managed:captcha:`— Wird verwendet, um über den Status der CAPTCHA-Informationen des Tokens zu berichten.

Token-Statusbezeichnungen: Labelnamen

Nach dem Präfix enthält der Rest des Labels detaillierte Informationen zum Token-Status:

- `accepted`— Das Anforderungstoken ist vorhanden und enthält Folgendes:
 - Eine gültige Challenge oder CAPTCHA-Lösung.
 - Eine noch nicht abgelaufene Herausforderung oder ein CAPTCHA-Zeitstempel.
 - Eine Domainspezifikation, die für die Web-ACL gültig ist.

Beispiel: Das Label `awsaf:managed:token:accepted` gibt an, dass das Token der Webanfragen eine gültige Challenge-Lösung, einen noch nicht abgelaufenen Challenge-Zeitstempel und eine gültige Domain enthält.

- `rejected`— Das Anforderungstoken ist vorhanden, erfüllt aber nicht die Akzeptanzkriterien.

Zusammen mit dem abgelehnten Label fügt die Tokenverwaltung einen benutzerdefinierten Label-Namespace und einen Namen hinzu, um den Grund anzugeben.

- `rejected:not_solved`— Dem Token fehlt die Challenge- oder CAPTCHA-Lösung.
- `rejected:expired`— Der Challenge- oder CAPTCHA-Zeitstempel des Tokens ist gemäß den von Ihrer Web-ACL konfigurierten Token-Immunitätszeiten abgelaufen.

- `rejected:domain_mismatch`— Die Domain des Tokens entspricht nicht der Token-Domain-Konfiguration Ihrer Web-ACL.
- `rejected:invalid`— Das angegebene Token AWS WAF konnte nicht gelesen werden.

Beispiel: Die Labels `awsaf:managed:captcha:rejected` und `awsaf:managed:captcha:rejected:expired` geben an, dass die Anfrage abgelehnt wurde, weil der CAPTCHA-Zeitstempel im Token die in der Web-ACL konfigurierte CAPTCHA-Token-Immunitätszeit überschritten hat.

- `absent`— Die Anfrage hat das Token nicht oder der Token-Manager konnte es nicht lesen.

Beispiel: Das Label `awsaf:managed:captcha:absent` gibt an, dass die Anfrage das Token nicht enthält.

Anfragen blockieren, die kein gültiges Token haben

Wenn Sie die Regelgruppen „AWS Managed Rules“ für intelligente Bedrohungen verwenden `AWSManagedRulesACFPRuleSet` `AWSManagedRulesATPRuleSet`, rufen die Regelgruppen die AWS WAF Tokenverwaltung auf `AWSManagedRulesBotControlRuleSet`, um den Status des Webanforderungstokens auszuwerten und die Anfragen entsprechend zu kennzeichnen.

Note

Die Token-Kennzeichnung wird nur auf Webanfragen angewendet, die Sie mithilfe einer dieser verwalteten Regelgruppen auswerten.

Informationen zur Kennzeichnung, die von der Tokenverwaltung angewendet wird, finden Sie im vorherigen Abschnitt, [Token-Kennzeichnung durch die verwalteten Regelgruppen zur intelligenten Bedrohungsabwehr](#).

Die verwalteten Regelgruppen zur intelligenten Bedrohungsabwehr behandeln die Token-Anforderungen dann wie folgt:

- Die `AWSManagedRulesACFPRuleSet` `AllRequests` Regel ist so konfiguriert, dass sie die Challenge Aktion für alle Anfragen ausführt und somit alle Anfragen blockiert, die nicht über das `accepted` Token-Label verfügen.
- Die `AWSManagedRulesATPRuleSet` blockiert Anfragen mit dem `rejected` Token-Label, blockiert aber keine Anfragen mit dem `absent` Token-Label.

- Die `AWSManagedRulesBotControlRuleSet` angestrebte Schutzstufe stellt Clients vor Herausforderungen, nachdem sie fünf Anfragen ohne `accepted` Token-Label gesendet haben. Es blockiert keine einzelne Anfrage, die kein gültiges Token hat. Die allgemeine Schutzzebene der Regelgruppe verwaltet die Tokenanforderungen nicht.

Weitere Informationen zu den Regelgruppen für intelligente Bedrohungen finden Sie [AWS WAF Regelgruppe Betrugsprävention \(ACFP\) zur Kontoerstellung bei der Betrugsbekämpfung](#) unter [AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen \(ATP\) zur Betrugsbekämpfung](#) und [AWS WAF Regelgruppe „Bot-Kontrolle“](#).

So blockieren Sie Anfragen, bei denen Token fehlen, wenn Sie die von Bot Control oder ATP verwaltete Regelgruppe verwenden

Mit den Regelgruppen Bot Control und ATP ist es möglich, dass eine Anfrage ohne gültiges Token die Regelgruppen-Evaluierung beendet und weiterhin von der Web-ACL ausgewertet wird.

Um alle Anfragen zu blockieren, deren Token fehlt oder deren Token abgelehnt wurde, fügen Sie eine Regel hinzu, die unmittelbar nach der verwalteten Regelgruppe ausgeführt wird, um Anfragen zu erfassen und zu blockieren, die die Regelgruppe nicht für Sie bearbeitet.

Im Folgenden finden Sie ein Beispiel für eine JSON-Liste für eine Web-ACL, die die verwaltete ATP-Regelgruppe verwendet. Der Web-ACL wurde eine Regel hinzugefügt, um das `awswaf:managed:token:absent` Label zu erfassen und zu verarbeiten. Die Regel schränkt ihre Auswertung auf Webanfragen ein, die an den Anmeldeendpunkt gehen, um dem Geltungsbereich der ATP-Regelgruppe zu entsprechen. Die hinzugefügte Regel ist fett gedruckt.

```
{
  "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": "awsaf: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": "aws-waf-111111111111:webacl:exampleWebACL:"
}
```

Konfiguration erforderlich für Application Load Balancer, die Origins sind CloudFront

Lesen Sie diesen Abschnitt, wenn Sie Ihre Web-ACL einem Application Load Balancer zuordnen und den Application Load Balancer als Ursprung für eine CloudFront Distribution bereitstellen.

Bei dieser Architektur müssen Sie die folgende zusätzliche Konfiguration bereitstellen, damit die Token-Informationen korrekt verarbeitet werden.

- Konfigurieren Sie CloudFront, dass das `aws-waf-token` Cookie an den Application Load Balancer weitergeleitet wird. CloudFront entfernt standardmäßig Cookies aus der Webanfrage, bevor sie an den Ursprung weitergeleitet wird. Um das Token-Cookie zusammen mit der Webanforderung beizubehalten, konfigurieren Sie das CloudFront Cache-Verhalten so, dass entweder nur das Token-Cookie oder alle Cookies enthalten sind. Informationen dazu, wie Sie dies tun können, finden Sie im Amazon CloudFront Developer Guide unter [Zwischenspeichern von Inhalten auf Basis von Cookies](#).
- Konfigurieren Sie es AWS WAF so, dass die Domain der CloudFront Distribution als gültige Token-Domain erkannt wird. CloudFront setzt den Host Header standardmäßig auf den Application Load Balancer Ursprung und AWS WAF verwendet diesen als Domäne der geschützten Ressource. Der Client-Browser betrachtet die CloudFront Distribution jedoch als Hostdomäne, und Token, die für den Client generiert werden, verwenden die CloudFront Domäne als Tokendomäne. Wenn die geschützte Ressourcendomäne mit AWS WAF der Tokendomäne verglichen wird,

kommt es ohne zusätzliche Konfiguration zu einer Diskrepanz. Um dieses Problem zu beheben, fügen Sie den Namen der CloudFront Distributionsdomäne zur Liste der Tokendomänen in Ihrer Web-ACL-Konfiguration hinzu. Weitere Informationen über die entsprechende Vorgehensweise finden Sie unter [Konfiguration der Domainliste für Web-ACL-Tokens](#).

AWS WAF Einrichtung von Konten bei der Betrugsbekämpfung und Betrugsprävention (ACFP)

Betrug bei der Kontoerstellung ist eine illegale Online-Aktivität, bei der ein Angreifer versucht, ein oder mehrere gefälschte Konten zu erstellen. Angreifer verwenden gefälschte Konten für betrügerische Aktivitäten wie den Missbrauch von Werbe- und Anmeldeboni, das Ausgeben einer anderen Person und für Cyberangriffe wie Phishing. Das Vorhandensein gefälschter Konten kann sich negativ auf Ihr Unternehmen auswirken, da es Ihren Ruf bei Kunden schädigt und der Gefahr von Finanzbetrug ausgesetzt ist.

Sie können Betrugsversuche bei der Kontoerstellung überwachen und kontrollieren, indem Sie die Funktion AWS WAF Fraud Control Account Creation Fraud Prevention (ACFP) implementieren. AWS WAF bietet diese Funktion in der Regelgruppe „AWS Verwaltete Regeln“ `AWSManagedRulesACFPRuleSet` mit zugehörigen SDKs zur Anwendungsintegration an.

Die verwaltete Regelgruppe ACFP kennzeichnet und verwaltet Anfragen, die Teil böswilliger Versuche zur Kontoerstellung sein könnten. Zu diesem Zweck untersucht die Regelgruppe Versuche zur Kontoerstellung, die Clients an den Kontoanmeldeendpunkt Ihrer Anwendung senden.

ACFP schützt Ihre Kontoanmeldeseiten, indem es Anfragen zur Kontoregistrierung auf ungewöhnliche Aktivitäten überwacht und verdächtige Anfragen automatisch blockiert. Die Regelgruppe verwendet Anforderungskennungen, Verhaltensanalysen und maschinelles Lernen, um betrügerische Anfragen zu erkennen.

- Prüfung von Anfragen — ACFP gibt Ihnen Einblick und Kontrolle über ungewöhnliche Kontoerstellungsversuche und Versuche, bei denen gestohlene Anmeldeinformationen verwendet werden, um die Erstellung betrügerischer Konten zu verhindern. ACFP überprüft E-Mail- und Passwortkombinationen anhand seiner Datenbank mit gestohlenen Anmeldeinformationen, die regelmäßig aktualisiert wird, sobald neue durchgesickerte Anmeldeinformationen im Dark Web gefunden werden. ACFP bewertet die in E-Mail-Adressen verwendeten Domains und überwacht die Verwendung von Telefonnummern und Adressfeldern, um die Eingaben zu überprüfen und betrügerisches Verhalten aufzudecken. ACFP aggregiert Daten nach IP-Adresse und Clientsitzung, um Clients zu erkennen und zu blockieren, die zu viele Anfragen verdächtiger Art senden.

- Überprüfung der Antworten — Bei CloudFront Verteilungen überprüft die ACFP-Regelgruppe nicht nur eingehende Anfragen zur Kontoerstellung, sondern auch die Antworten Ihrer Anwendung auf Versuche zur Kontoerstellung, um Erfolgs- und Misserfolgsraten nachzuverfolgen. Mithilfe dieser Informationen kann ACFP vorübergehend Clientsitzungen oder IP-Adressen blockieren, bei denen zu viele Versuche fehlgeschlagen sind. AWS WAF führt die Antwortprüfung asynchron durch, sodass die Latenz Ihres Webverkehrs dadurch nicht erhöht wird.

Note

Ihnen werden zusätzliche Gebühren berechnet, wenn Sie diese verwaltete Regelgruppe verwenden. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).

Note

Die ACFP-Funktion ist für Amazon Cognito Cognito-Benutzerpools nicht verfügbar.

Themen


- [ACFP-Komponenten](#)
- [Warum sollten Sie die Anwendungsintegrations-SDKs mit ACFP verwenden](#)
- [Hinzufügen der verwalteten ACFP-Regelgruppe zu Ihrer Web-ACL](#)
- [Testen und Bereitstellen von ACFP](#)
- [AWS WAF Beispiele für die Einrichtung von Konten bei der Betrugsbekämpfung \(ACFP\)](#)

ACFP-Komponenten

Die Hauptkomponenten der AWS WAF Betrugsbekämpfung bei der Kontoerstellung und Betrugsprävention (ACFP) sind die folgenden:

- **AWSManagedRulesACFPRuleSet**— Die Regeln in dieser Regelgruppe „AWS Verwaltete Regeln“ erkennen, kennzeichnen und behandeln verschiedene Arten betrügerischer Aktivitäten bei der Kontoerstellung. Die Regelgruppe untersucht GET HTTP-Text-/HTML-Anfragen, die Kunden an den angegebenen Endpunkt für die Kontoregistrierung senden, sowie POST Webanfragen, die Kunden an den angegebenen Endpunkt für die Kontoregistrierung senden. Bei geschützten CloudFront

Verteilungen überprüft die Regelgruppe auch die Antworten, die die Verteilung auf Anfragen zur Kontoerstellung zurücksendet. Eine Liste der Regeln dieser Regelgruppe finden Sie unter [AWS WAF Regelgruppe Betrugsprävention \(ACFP\) zur Kontoerstellung bei der Betrugsbekämpfung](#). Sie nehmen diese Regelgruppe in Ihre Web-ACL auf, indem Sie eine Referenzanweisung für die verwaltete Regelgruppe verwenden. Informationen zur Verwendung dieser Regelgruppe finden Sie unter [Hinzufügen der verwalteten ACFP-Regelgruppe zu Ihrer Web-ACL](#).

 Note

Ihnen werden zusätzliche Gebühren berechnet, wenn Sie diese verwaltete Regelgruppe verwenden. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).

- Einzelheiten zu den Seiten zur Kontoregistrierung und Kontoerstellung Ihrer Anwendung — Sie müssen Informationen zu den Seiten zur Kontoregistrierung und Kontoerstellung angeben, wenn Sie die `AWSManagedRulesACFPRuleSet` Regelgruppe zu Ihrer Web-ACL hinzufügen. Auf diese Weise kann die Regelgruppe den Umfang der Anfragen, die sie prüft, einschränken und Webanfragen zur Kontoerstellung ordnungsgemäß validieren. Die Registrierungsseite muss GET Text-/HTML-Anfragen akzeptieren. Der Pfad zur Kontoerstellung muss Anfragen akzeptierenPOST. Die ACFP-Regelgruppe arbeitet mit Benutzernamen im E-Mail-Format. Weitere Informationen finden Sie unter [Hinzufügen der verwalteten ACFP-Regelgruppe zu Ihrer Web-ACL](#).
- Bei geschützten CloudFront Distributionen: Details darüber, wie Ihre Anwendung auf Versuche zur Kontoerstellung reagiert — Sie geben Details zu den Antworten Ihrer Anwendung auf Versuche zur Kontoerstellung an, und die ACFP-Regelgruppe verfolgt und verwaltet Versuche zur Erstellung mehrerer Konten von einer einzelnen IP-Adresse oder einer einzelnen Clientsitzung aus. Informationen zur Konfiguration dieser Option finden Sie unter [Hinzufügen der verwalteten ACFP-Regelgruppe zu Ihrer Web-ACL](#).
- JavaScript und SDKs für die Integration mobiler Anwendungen — Implementieren Sie die SDKs AWS WAF JavaScript und die mobilen SDKs zusammen mit Ihrer ACFP-Implementierung, um alle Funktionen zu nutzen, die die Regelgruppe bietet. Viele der ACFP-Regeln verwenden die von den SDKs bereitgestellten Informationen für die Client-Überprüfung auf Sitzungsebene und die Aggregation von Verhalten, die erforderlich sind, um legitimen Client-Verkehr vom Bot-Verkehr zu trennen. Weitere Informationen zu den SDKs finden Sie unter [AWS WAF Integration von Client-Anwendungen](#).

Sie können Ihre ACFP-Implementierung mit den folgenden Komponenten kombinieren, um Ihre Schutzmaßnahmen zu überwachen, zu optimieren und anzupassen.

- **Protokollierung und Metriken** — Sie können Ihren Datenverkehr überwachen und verstehen, wie sich die von ACFP verwaltete Regelgruppe darauf auswirkt, indem Sie Logs und CloudWatch Amazon-Metriken für Ihre Web-ACL konfigurieren und aktivieren. Die Labels, die Ihren Webanfragen `AWSManagedRulesACFPRuleSet` hinzugefügt werden, sind in den Protokollen und in den CloudWatch Amazon-Metriken enthalten. Informationen zu Protokollierung und Metriken finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#) und [Überwachung mit Amazon CloudWatch](#).

Abhängig von Ihren Anforderungen und dem Datenverkehr, den Sie beobachten, möchten Sie Ihre `AWSManagedRulesACFPRuleSet`-Implementierung möglicherweise anpassen. Beispielsweise möchten Sie möglicherweise einen Teil des Datenverkehrs von der ACFP-Auswertung ausschließen oder die Art und Weise ändern, wie das Unternehmen mit einigen der von ihr identifizierten Betrugsversuche bei der Kontoerstellung umgeht, und zwar mithilfe von AWS WAF Funktionen wie Scopedown-Aussagen oder Regeln für den Label-Abgleich.

- **Bezeichnungen und Regeln zum Abgleich von Bezeichnungen** – Für jede der Regeln in `AWSManagedRulesACFPRuleSet` können Sie das Blockierverhalten auf „Zählen“ umstellen und dann mit den Bezeichnungen abgleichen, die durch die Regeln hinzugefügt wurden. Verwenden Sie diesen Ansatz, um anzupassen, wie Sie mit Webanfragen umgehen, die von der verwalteten ACFP-Regelgruppe identifiziert werden. Weitere Informationen zur Bezeichnung und zur Verwendung von Anweisungen zum Abgleich von Bezeichnungen finden Sie unter [Regelanweisung für Bezeichnungsübereinstimmung](#) und [AWS WAF Labels auf Webanfragen](#).
- **Benutzerdefinierte Anforderungen und Antworten** – Sie können den Anforderungen, die Sie zulassen, benutzerdefinierte Header hinzufügen, und Sie können für blockierte Anforderungen benutzerdefinierte Antworten senden. Dazu kombinieren Sie den Bezeichnungsabgleich mit den AWS WAF -Funktionen für benutzerdefinierte Anforderungen und Antworten. Weitere Informationen zum Anpassen von Anforderungen und Antworten finden Sie unter [Benutzerdefinierte Webanforderungen und Antworten in AWS WAF](#).

Warum sollten Sie die Anwendungsintegrations-SDKs mit ACFP verwenden

Wir empfehlen dringend, die Anwendungsintegrations-SDKs zu implementieren, um die ACFP-Regelgruppe am effizientesten nutzen zu können.

- **Vollständige Regelgruppenfunktionalität** — Die ACFP-Regel funktioniert `SignalClientInteractivityAbsentLow` nur mit Token, die von den Anwendungsintegrationen aufgefüllt werden. Diese Regel erkennt und verwaltet abnormale menschliche Interaktivitäten mit der Anwendungsseite. Die Anwendungsintegrations-SDKs können

normale menschliche Interaktivität durch Mausbewegungen, Tastendrucke und andere Messungen erkennen. Die Interstitials, die von den Regelaktionen gesendet werden CAPTCHA und diese Art von Daten nicht bereitstellen Challenge können.

- **Reduzierte Latenz** — Die Regelgruppenregel `AllRequests` wendet die Challenge Regelaktion auf jede Anfrage an, für die noch kein Challenge-Token vorhanden ist. In diesem Fall wird die Anfrage von der Regelgruppe zweimal ausgewertet: einmal ohne das Token und dann ein zweites Mal, nachdem das Token mithilfe der Challenge Aktion `Interstitial` abgerufen wurde. Ihnen werden keine zusätzlichen Gebühren berechnet, wenn Sie nur die `AllRequests` Regel verwenden, aber dieser Ansatz erhöht den Overhead Ihres Web-Traffics und erhöht die Latenz Ihrer Endbenutzererfahrung. Wenn Sie das Token clientseitig mithilfe der Anwendungsintegrationen erwerben, bevor Sie die Anfrage zur Kontoerstellung senden, wertet die `ACFP`-Regelgruppe die Anfrage einmal aus.

Weitere Informationen zu den Funktionen der Regelgruppe finden Sie unter [AWS WAF Regelgruppe Betrugsprävention \(ACFP\) zur Kontoerstellung bei der Betrugsbekämpfung](#)

Informationen zu den SDKs finden Sie unter [AWS WAF Integration von Client-Anwendungen](#).

Informationen zu AWS WAF Tokens finden Sie unter [AWS WAF Webanforderungstoken](#).

Informationen zu den Regelaktionen finden Sie unter [CAPTCHA und Challenge in AWS WAF](#).

Hinzufügen der verwalteten ACFP-Regelgruppe zu Ihrer Web-ACL

Um die verwaltete ACFP-Regelgruppe so zu konfigurieren, dass betrügerische Aktivitäten bei der Kontoerstellung in Ihrem Web-Traffic erkannt werden, geben Sie Informationen darüber an, wie Kunden auf Ihre Registrierungsseite zugreifen, und senden Anfragen zur Kontoerstellung an Ihre Anwendung. Für geschützte CloudFront Amazon-Distributionen geben Sie auch Informationen darüber an, wie Ihre Anwendung auf Anfragen zur Kontoerstellung reagiert. Diese Konfiguration gilt zusätzlich zur normalen Konfiguration für eine verwaltete Regelgruppe.

Eine Beschreibung der Regelgruppe und eine Liste der Regeln finden Sie unter [AWS WAF Regelgruppe Betrugsprävention \(ACFP\) zur Kontoerstellung bei der Betrugsbekämpfung](#).

Note

Die Datenbank mit gestohlenen ACFP-Anmeldeinformationen enthält nur Benutzernamen im E-Mail-Format.


Diese Anleitung richtet sich an Benutzer, die im Allgemeinen wissen, wie man Web-ACLs, Regeln und Regelgruppen für AWS WAF erstellt und verwaltet. Diese Themen werden in früheren Abschnitten dieses Handbuchs behandelt. Grundlegende Informationen zum Hinzufügen einer verwalteten Regelgruppe zu einer Web-ACL finden Sie unter [Hinzufügen einer verwalteten Regelgruppe zu einer Web-ACL über die Konsole](#).

Folgen Sie den bewährten Methoden

Verwenden Sie die ACFP-Regelgruppe gemäß den bewährten Methoden unter [Bewährte Methoden für intelligente Bedrohungsabwehr](#).

So verwenden Sie die Regelgruppe **AWSManagedRulesACFPRuleSet** in einer Web-ACL

1. Fügen Sie die AWS verwaltete Regelgruppe **AWSManagedRulesACFPRuleSet** zu Ihrer Web-ACL hinzu und bearbeiten Sie die Regelgruppeneinstellungen vor dem Speichern.

 Note

Ihnen werden zusätzliche Gebühren berechnet, wenn Sie diese verwaltete Regelgruppe verwenden. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).

2. Geben Sie im Bereich Regelgruppenkonfiguration die Informationen ein, anhand derer die ACFP-Regelgruppe Anfragen zur Kontoerstellung prüft.
 - a. Aktivieren Sie diese Option für Reguläre Ausdrücke in Pfaden verwenden, wenn Sie einen Abgleich mit regulären Ausdrücken für die Pfadspezifikationen Ihrer Registrierungs- und Kontoerstellungssseite durchführen möchten AWS WAF .

AWS WAF unterstützt `libpcre` mit einigen Ausnahmen die von der PCRE-Bibliothek verwendete Mustersyntax. Die Bibliothek ist unter [PCRE - Perl Compatible Regular Expressions](#) (Perl-kompatible reguläre Ausdrücke) dokumentiert. Hinweise zur AWS WAF Unterstützung finden Sie unter [Musterabgleich mit regulären Ausdrücken in AWS WAF](#).

- b. Geben Sie unter Pfad zur Registrierungsseite den Pfad zum Endpunkt der Registrierungsseite für Ihre Anwendung an. Diese Seite muss GET Text-/HTML-Anfragen akzeptieren. Die Regelgruppe untersucht nur GET HTTP-Text-/HTML-Anfragen an den von Ihnen angegebenen Endpunkt der Registrierungsseite.

Note

Beim Abgleich für Endpunkte wird nicht zwischen Groß- und Kleinschreibung unterschieden. Regex-Spezifikationen dürfen das Flag nicht enthalten(`?-i`), wodurch der Abgleich ohne Berücksichtigung der Groß- und Kleinschreibung deaktiviert wird. Zeichenkettenspezifikationen müssen mit einem Schrägstrich beginnen. /

Für die URL könnten Sie `https://example.com/web/registration` beispielsweise die Pfadangabe `/web/registration` für die Zeichenfolge angeben. Pfade auf Registrierungsseiten, die mit dem von Ihnen angegebenen Pfad beginnen, werden als übereinstimmend betrachtet. `/web/registration` Entspricht beispielsweise den `/web/registration` Registrierungspfaden `/web/registration//web/registrationPage`, und `/web/registration/thisPage`, entspricht aber nicht dem Pfad `/home/web/registration` oder `/website/registration`.

Note

Stellen Sie sicher, dass Ihre Endbenutzer die Registrierungsseite laden, bevor sie eine Anfrage zur Kontoerstellung einreichen. Dadurch wird sichergestellt, dass die Anfragen des Kunden zur Kontoerstellung gültige Token enthalten.


- c. Geben Sie als Pfad zur Kontoerstellung die URI auf Ihrer Website an, die vollständige neue Benutzerdaten akzeptiert. Diese URI muss POST Anfragen akzeptieren.

Note

Beim Abgleich für Endpunkte wird nicht zwischen Groß- und Kleinschreibung unterschieden. Regex-Spezifikationen dürfen das Flag nicht enthalten(`?-i`), wodurch der Abgleich ohne Berücksichtigung der Groß- und Kleinschreibung deaktiviert wird. Zeichenkettenspezifikationen müssen mit einem Schrägstrich beginnen. /

Für die URL könnten Sie `https://example.com/web/newaccount` beispielsweise die Pfadangabe `/web/newaccount` für die Zeichenfolge angeben. Pfade zur Kontoerstellung, die mit dem von Ihnen angegebenen Pfad beginnen, werden als übereinstimmend betrachtet. `/web/newaccount` entspricht beispielsweise den Pfaden zur Kontoerstellung `/web/newaccount`, `/web/newaccount//web/newaccountPage`, `/web/newaccount/thisPage`, und, entspricht aber nicht dem Pfad `/home/web/newaccount` oder `website/newaccount`.

- d. Geben Sie für die Prüfung von Anfragen an, wie Ihre Anwendung Versuche zur Kontoerstellung akzeptiert, indem Sie den Payload-Typ der Anfrage und die Namen der Felder im Anfragetext angeben, in denen der Benutzername, das Passwort und andere Details zur Kontoerstellung angegeben werden.

 Note

Geben Sie für die Felder „Primäre Adresse“ und „Telefonnummer“ die Felder in der Reihenfolge an, in der sie in der Payload der Anfrage erscheinen.

Ihre Angabe der Feldnamen hängt vom Payload-Typ ab.

- JSON-Nutzdatentyp — Geben Sie die Feldnamen in der JSON-Zeigersyntax an. Informationen zur JSON-Pointer-Syntax finden Sie in der Dokumentation [JavaScriptObject Notation \(JSON\) Pointer der Internet Engineering Task Force \(IETF\)](#).

Für die folgende Beispiel-JSON-Nutzlast lautet die Feldspezifikation für den Benutzernamen, `/signupform/username` und die Spezifikationen für das primäre Adressfeld lauten `/signupform/addrp1/signupform/addrp2`, und `/signupform/addrp3`


```
{
  "signupform": {
    "username": "THE_USERNAME",
    "password": "THE_PASSWORD",
    "addrp1": "PRIMARY_ADDRESS_LINE_1",
    "addrp2": "PRIMARY_ADDRESS_LINE_2",
    "addrp3": "PRIMARY_ADDRESS_LINE_3",
    "phonecode": "PRIMARY_PHONE_CODE",
```

```
    "phonenumber": "PRIMARY_PHONE_NUMBER"  
  }  
}
```

- Payload-Typ FORM_ENCODED — Verwenden Sie die HTML-Formularnamen.

Für ein HTML-Formular mit Benutzer- und Kennworteingabelementen mit dem Namen `username1` und `password1` lautet die Feldspezifikation für den Benutzernamen `username1` und die Feldspezifikation für das Passwort. `password1`

- e. Wenn Sie CloudFront Amazon-Distributionen schützen, geben Sie unter Überprüfung von Antworten an, wie Ihre Anwendung bei den Antworten auf Versuche zur Kontoerstellung auf Erfolg oder Misserfolg reagiert.

 Note

ACFP Response Inspection ist nur in Web-ACLs verfügbar, die Distributionen schützen. CloudFront

Geben Sie in der Antwort auf die Kontoerstellung eine einzelne Komponente an, die ACFP überprüfen soll. AWS WAF Kann bei den Komponententypen Body und JSON die ersten 65.536 Byte (64 KB) der Komponente untersuchen.

Geben Sie Ihre Prüfkriterien für den Komponententyp an, wie in der Schnittstelle angegeben. Sie müssen sowohl Erfolgs- als auch Fehlschlagskriterien angeben, nach denen die Komponente geprüft werden soll.

Angenommen, Ihre Anwendung gibt im Statuscode der Antwort den Status eines Versuchs zur Kontoerstellung an und verwendet ihn `200 OK` für Erfolg `401 Unauthorized` und/oder `403 Forbidden` für Fehlschlag. Sie würden den Komponententyp der Antwortprüfung auf Statuscode setzen und dann in das Textfeld Erfolg `200` und im Textfeld Fehler den Text in `401` der ersten Zeile und in `403` der zweiten Zeile eingeben.

Die ACFP-Regelgruppe zählt nur Antworten, die Ihren Erfolgs- oder Fehlschlagprüfkriterien entsprechen. Die Regelgruppenregeln wirken sich auf Kunden aus, deren Erfolgsquote unter den gezählten Antworten zu hoch ist, um Versuche, mehrere Konten zu erstellen, zu verhindern. Stellen Sie sicher, dass Sie vollständige Informationen zu erfolgreichen und fehlgeschlagenen Kontoerstellungsversuchen angeben, damit sich die Regelgruppenregeln korrekt verhalten.

Die Regeln zur Überprüfung der Antworten auf die Kontoerstellung finden Sie `VolumeMetricSessionSuccessfulResponse` in der Regelliste unter [AWS WAF Regelgruppe Betrugsprävention \(ACFP\) zur Kontoerstellung bei der Betrugsbekämpfung](#). `VolumeMetricIPSuccessfulResponse`

3. Geben Sie jede zusätzliche Konfiguration an, die für die Regelgruppe benötigt wird.

Sie können den Umfang der Anforderungen, die von der Regelgruppe geprüft werden, weiter eingrenzen, indem Sie der Anweisung für die verwaltete Regelgruppe eine Eingrenzungsanweisung hinzufügen. So können Sie beispielsweise nur Anforderungen mit einem bestimmten Abfrageargument oder Cookie prüfen. Die Regelgruppe prüft nur Anfragen, die den Kriterien in Ihrer Zusammenfassung entsprechen und die an die von Ihnen in der Regelgruppenkonfiguration angegebenen Pfade zur Kontoregistrierung und Kontoerstellung gesendet werden. Informationen zu Eingrenzungsanweisungen finden Sie unter [Eingrenzungsanweisungen](#).

4. Speichern Sie Ihre Änderungen an der Web-ACL.

Bevor Sie Ihre ACFP-Implementierung für den Produktionsdatenverkehr einsetzen, testen und optimieren Sie sie in einer Staging- oder Testumgebung, bis Sie mit den möglichen Auswirkungen auf Ihren Datenverkehr zufrieden sind. Testen und optimieren Sie dann die Regeln im Zählmodus mit Ihrem Produktionsdatenverkehr, bevor Sie sie aktivieren. Anleitungen finden Sie im folgenden Abschnitt.

Testen und Bereitstellen von ACFP

Dieser Abschnitt enthält allgemeine Anleitungen zur Konfiguration und zum Testen einer Implementierung zur AWS WAF Betrugsbekämpfung (Fraud Control Account Creation Fraud Prevention, ACFP) für Ihre Website. Für welche Schritte Sie sich im Einzelnen entscheiden, hängt von Ihren Anforderungen, Ihren Ressourcen und den bei Ihnen eingehenden Webanforderungen ab.

Diese Informationen ergänzen die allgemeinen Informationen zum Testen und Optimieren unter [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

Note

AWS Verwaltete Regeln wurden entwickelt, um Sie vor gängigen Internet-Bedrohungen zu schützen. Wenn sie gemäß der Dokumentation verwendet werden, bieten Regelgruppen mit AWS verwalteten Regeln eine weitere Sicherheitsebene für Ihre Anwendungen.

Regelgruppen mit AWS verwalteten Regeln sind jedoch nicht als Ersatz für Ihre Sicherheitsaufgaben gedacht, die durch die von Ihnen ausgewählten AWS Ressourcen bestimmt werden. Anhand des [Modells der gemeinsamen Verantwortung](#) können Sie sicherstellen, dass Ihre Ressourcen ordnungsgemäß geschützt AWS sind.

Risiken rund um Produktionsdatenverkehr

Bevor Sie Ihre ACFP-Implementierung für den Produktionsdatenverkehr einsetzen, testen und optimieren Sie sie in einer Staging- oder Testumgebung, bis Sie mit den möglichen Auswirkungen auf Ihren Datenverkehr zufrieden sind. Testen und optimieren Sie dann die Regeln im Zählmodus mit Ihrem Produktionsdatenverkehr, bevor Sie sie aktivieren.

AWS WAF stellt Testanmeldedaten bereit, mit denen Sie Ihre ACFP-Konfiguration überprüfen können. Im folgenden Verfahren konfigurieren Sie eine Test-Web-ACL für die Verwendung der verwalteten ACFP-Regelgruppe, konfigurieren eine Regel, die das von der Regelgruppe hinzugefügte Label erfasst, und führen dann mit diesen Testanmeldedaten einen Versuch durch, ein Konto zu erstellen. Sie überprüfen, ob Ihre Web-ACL den Versuch ordnungsgemäß bewilligt hat, indem Sie die CloudWatch Amazon-Metriken für den Versuch der Kontoerstellung überprüfen.

Diese Anleitung richtet sich an Benutzer, die im Allgemeinen wissen, wie man Web-ACLs, Regeln und Regelgruppen für AWS WAF erstellt und verwaltet. Diese Themen werden in früheren Abschnitten dieses Handbuchs behandelt.

Um eine ACFP-Implementierung (AWS WAF Fraud Control Account Creation Fraud Prevention) zu konfigurieren und zu testen

Führen Sie diese Schritte zuerst in einer Testumgebung und dann in der Produktion aus.

1. Fügen Sie die AWS WAF verwaltete Regelgruppe zur Erstellung von Fraud Control-Konten und Fraud Prevention (ACFP) im Zählmodus hinzu

Note

Ihnen werden zusätzliche Gebühren berechnet, wenn Sie diese verwaltete Regelgruppe verwenden. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).

Fügen Sie die Regelgruppe `AWManagedRulesACFPRuleSet` „AWS Verwaltete Regeln“ einer neuen oder vorhandenen Web-ACL hinzu und konfigurieren Sie sie so, dass sie das aktuelle Verhalten der Web-ACL nicht verändert. Weitere Informationen zu den Regeln und Bezeichnungen für diese Regelgruppe finden Sie unter [AWS WAF Regelgruppe Betrugsprävention \(ACFP\) zur Kontoerstellung bei der Betrugsbekämpfung](#).

- Wenn Sie die verwaltete Regelgruppe hinzufügen, bearbeiten Sie sie und gehen Sie wie folgt vor:
 - Geben Sie im Bereich „Konfiguration der Regelgruppe“ die Details zu den Seiten zur Kontoregistrierung und Kontoerstellung Ihrer Anwendung ein. Die ACFP-Regelgruppe verwendet diese Informationen zur Überwachung der Anmeldeaktivitäten. Weitere Informationen finden Sie unter [Hinzufügen der verwalteten ACFP-Regelgruppe zu Ihrer Web-ACL](#).
 - Öffnen Sie im Bereich Regeln die Dropdownliste Alle Regelaktionen außer Kraft setzen und wählen Sie aus. Count Mit dieser Konfiguration wertet AWS WAF Anforderungen nach allen Regeln in der Regelgruppe aus und zählt nur die daraus resultierenden Übereinstimmungen. Gleichzeitig werden weiterhin Beschriftungen zu Anforderungen hinzugefügt. Weitere Informationen finden Sie unter [Regelaktionen in einer Regelgruppe überschreiben](#).

Mit dieser Außerkräftsetzung können Sie die potenziellen Auswirkungen der von ACFP verwalteten Regeln überwachen und entscheiden, ob Sie Ausnahmen hinzufügen möchten, z. B. Ausnahmen für interne Anwendungsfälle.

- Positionieren Sie die Regelgruppe so, dass sie nach Ihren vorhandenen Regeln in der Web-ACL ausgewertet wird, mit einer Prioritätseinstellung, die numerisch höher ist als alle Regeln oder Regelgruppen, die Sie bereits verwenden. Weitere Informationen finden Sie unter [Reihenfolge der Verarbeitung von Regeln und Regelgruppen in einer Web-ACL](#).

Auf diese Weise wird Ihre derzeitige Handhabung des Datenverkehrs nicht gestört. Wenn Sie beispielsweise Regeln haben, die bösartigen Datenverkehr wie SQL-Injections oder Cross-Site-Scripting erkennen, erkennen und protokollieren sie diese Probleme weiterhin. Wenn Sie Regeln haben, die bekannten, nicht böswilligen Datenverkehr zulassen, können diese Regeln diesen Datenverkehr auch weiterhin zulassen, ohne dass er von der von ACFP verwalteten Regelgruppe blockiert wird. Möglicherweise entscheiden Sie sich, die Verarbeitungsreihenfolge während Ihrer Test- und Optimierungsaktivitäten anzupassen.

2. Implementieren Sie die Anwendungsintegrations-SDKs

Integrieren Sie das AWS WAF JavaScript SDK in die Kontoregistrierungs- und Kontoerstellungspfade Ihres Browsers. AWS WAF bietet auch mobile SDKs zur Integration von iOS- und Android-Geräten. Weitere Informationen zum den Integrations-SDKs finden Sie unter [AWS WAF Integration von Client-Anwendungen](#). Informationen zu dieser Empfehlung finden Sie unter [Warum sollten Sie die Anwendungsintegrations-SDKs mit ACFP verwenden](#).

Note

Wenn Sie die Anwendungsintegrations-SDKs nicht verwenden können, können Sie die ACFP-Regelgruppe testen, indem Sie sie in Ihrer Web-ACL bearbeiten und die Überschreibung entfernen, die Sie der `AllRequests` Regel zugewiesen haben. Dadurch wird die Challenge Aktionseinstellung der Regel aktiviert, um sicherzustellen, dass Anfragen ein gültiges Challenge-Token enthalten.

Tun Sie dies zuerst in einer Testumgebung und dann mit größter Sorgfalt in Ihrer Produktionsumgebung. Dieser Ansatz hat das Potenzial, Benutzer zu blockieren. Wenn der Pfad Ihrer Registrierungsseite beispielsweise keine GET Text-/HTML-Anfragen akzeptiert, kann diese Regelkonfiguration effektiv alle Anfragen auf der Registrierungsseite blockieren.

3. Aktivieren von Sampling, Protokollierung und Metriken für die Web-ACL

Konfigurieren Sie bei Bedarf die Protokollierung für die Web-ACL und aktivieren Sie Sampling und CloudWatch Amazon-Metriken. Sie können diese Sichtbarkeitstools verwenden, um die Interaktion der von ACFP verwalteten Regelgruppe mit Ihrem Datenverkehr zu überwachen.

- Weitere Informationen zum Konfigurieren und Verwenden der Protokollierung finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).
- Informationen zu CloudWatch Amazon-Metriken finden Sie unter [Überwachung mit Amazon CloudWatch](#).
- Informationen zum Sampling von Webanforderungen finden Sie unter [Anzeigen einer Stichprobe von Webanforderungen](#).

4. Zuordnen der Web-ACL zu einer Ressource

Wenn die Web-ACL noch keiner Testressource zugeordnet ist, ordnen Sie sie zu. Weitere Informationen finden Sie unter [Zuordnen oder Aufheben der Zuordnung einer Web-ACL zu einer Ressource AWS](#).

5. Überwachen Sie den Datenverkehr und die Übereinstimmung mit den ACFP-Regeln

Stellen Sie sicher, dass Ihr normaler Datenverkehr fließt und dass die Regeln für verwaltete ACFP-Regelgruppen übereinstimmende Webanfragen mit Labels versehen. Sie können die Labels in den Protokollen und die ACFP- und Label-Metriken in den CloudWatch Amazon-Metriken sehen. In den Protokollen werden die Regeln, die Sie zur Zählung in der Regelgruppe außer Kraft gesetzt haben, in der Liste mit auf zählen `action` gesetzt und `ruleGroupList` mit der `overriddenAction` Angabe der konfigurierten Regelaktion angezeigt, die Sie überschrieben haben.

6. Testen der Regelgruppenfunktionen zur Überprüfung von Anmeldeinformationen

Führen Sie einen Versuch zur Kontoerstellung mit manipulierten Testanmeldedaten durch und überprüfen Sie, ob die Regelgruppe erwartungsgemäß mit ihnen übereinstimmt.

- a. Rufen Sie die Kontoregistrierungsseite Ihrer geschützten Ressource auf und versuchen Sie, ein neues Konto hinzuzufügen. Verwenden Sie das folgende Paar AWS WAF Testanmeldeinformationen und geben Sie einen beliebigen Test ein

- Benutzer: `WAF_TEST_CREDENTIAL@wafexample.com`
- Passwort: `WAF_TEST_CREDENTIAL_PASSWORD`

Diese Testanmeldedaten werden als kompromittierte Anmeldeinformationen eingestuft, und die von ACFP verwaltete Regelgruppe fügt der Anfrage zur Kontoerstellung die `aws:waf:managed:aws:acfp:signal:credential_compromised` Bezeichnung hinzu, die Sie in den Protokollen sehen können.

- b. Suchen Sie in Ihren Web-ACL-Protokollen nach der `aws:waf:managed:aws:acfp:signal:credential_compromised` Bezeichnung im `labels` Feld in den Protokolleinträgen für Ihre Anfrage zur Erstellung eines Testkontos. Weitere Informationen zur Protokollierung finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).

Nachdem Sie sich vergewissert haben, dass die Regelgruppe kompromittierte Anmeldeinformationen wie erwartet erfasst, können Sie Maßnahmen ergreifen, um die Implementierung für Ihre geschützte Ressource nach Bedarf zu konfigurieren.

7. Testen Sie bei CloudFront Verteilungen, wie die Regelgruppe versucht, mehrere Konten gleichzeitig zu erstellen

Führen Sie diesen Test für jedes Erfolgskriterium aus, das Sie für die ACFP-Regelgruppe konfiguriert haben. Warten Sie zwischen den Tests mindestens 30 Minuten.

- a. Identifizieren Sie für jedes Ihrer Erfolgskriterien einen Versuch, ein Konto zu erstellen, der mit diesen Erfolgskriterien in der Antwort erfolgreich sein wird. Führen Sie dann von einer einzigen Kundensitzung aus mindestens 5 erfolgreiche Versuche zur Kontoerstellung in weniger als 30 Minuten durch. Ein Benutzer würde normalerweise nur ein einziges Konto auf Ihrer Site erstellen.

Nach der ersten erfolgreichen Kontoerstellung sollte die `VolumetricSessionSuccessfulResponse` Regel beginnen, sie mit den übrigen Antworten auf die Kontoerstellung abzugleichen, sie zu kennzeichnen und zu zählen, je nachdem, welche Regelaktion Sie außer Kraft gesetzt haben. Bei der Regel fehlen aufgrund der Latenz möglicherweise die ersten ein oder zwei Antworten.

- b. Suchen Sie in Ihren Web-ACL-Protokollen nach der `awsaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_1` Bezeichnung im `labels` Feld in den Protokolleinträgen für Ihre Webanfragen zur Erstellung von Testkonten. Weitere Informationen zur Protokollierung finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).

Diese Tests überprüfen, ob Ihre Erfolgskriterien mit Ihren Antworten übereinstimmen, indem geprüft wird, ob die Anzahl der erfolgreichen Ergebnisse, die durch die Regel aggregiert wurden, den Schwellenwert der Regel überschreitet. Wenn Sie nach Erreichen des Schwellenwerts weiterhin Anfragen zur Kontoerstellung aus derselben Sitzung senden, gilt die Regel weiterhin, bis die Erfolgsquote unter den Schwellenwert fällt. Solange der Schwellenwert überschritten ist, berücksichtigt die Regel sowohl erfolgreiche als auch fehlgeschlagene Kontoerstellungsversuche von der Sitzungsadresse aus.

8. Passen Sie die Behandlung von ACFP-Webanfragen an

Fügen Sie nach Bedarf Ihre eigenen Regeln hinzu, die Anfragen explizit zulassen oder blockieren, um zu ändern, wie ACFP-Regeln sie sonst behandeln würden.

Beispielsweise können Sie ACFP-Labels verwenden, um Anfragen zuzulassen oder zu blockieren oder die Bearbeitung von Anfragen anzupassen. Sie können hinter der verwalteten

ACFP-Regelgruppe eine Regel für den Label-Abgleich hinzufügen, um markierte Anfragen nach der Bearbeitung zu filtern, die Sie anwenden möchten. Behalten Sie nach dem Testen die zugehörigen ACFP-Regeln im Zählmodus bei und behalten Sie die Entscheidungen zur Bearbeitung von Anfragen in Ihrer benutzerdefinierten Regel bei. Ein Beispiel finden Sie unter [ACFP-Beispiel: Benutzerdefinierte Antwort auf kompromittierte Anmeldeinformationen](#).

9. Entfernen Sie Ihre Testregeln und aktivieren Sie die Einstellungen für verwaltete ACFP-Regelgruppen

Abhängig von Ihrer Situation haben Sie sich möglicherweise entschieden, einige ACFP-Regeln im Zählmodus zu belassen. Für die Regeln, die Sie wie in der Regelgruppe konfiguriert ausführen möchten, deaktivieren Sie den Zählmodus in der Web-ACL-Regelgruppenkonfiguration. Wenn Sie mit dem Testen fertig sind, können Sie auch Ihre Testlabel-Vergleichsregeln entfernen.

10. Überwachen und Anpassen

Um sicherzustellen, dass Webanfragen wie gewünscht bearbeitet werden, sollten Sie Ihren Datenverkehr genau beobachten, nachdem Sie die ACFP-Funktionalität aktiviert haben, die Sie verwenden möchten. Passen Sie das Verhalten nach Bedarf mit der Überschreibung der Regelzählung für die Regelgruppe und mit Ihren eigenen Regeln an.

Wenn Sie das AWS WAF JavaScript SDK nach Abschluss des Tests Ihrer ACFP-Regelgruppenimplementierung noch nicht in die Seiten zur Kontoregistrierung und Kontoerstellung Ihres Browsers integriert haben, empfehlen wir Ihnen dringend, dies zu tun. AWS WAF bietet auch mobile SDKs zur Integration von iOS- und Android-Geräten. Weitere Informationen zum den Integrations-SDKs finden Sie unter [AWS WAF Integration von Client-Anwendungen](#). Informationen zu dieser Empfehlung finden Sie unter [Warum sollten Sie die Anwendungsintegrations-SDKs mit ACFP verwenden](#).

AWS WAF Beispiele für die Einrichtung von Konten bei der Betrugsbekämpfung (ACFP)

Dieser Abschnitt zeigt Beispielkonfigurationen, die den gängigen Anwendungsfällen für die Implementierung von AWS WAF Fraud Control Account Creation Fraud Prevention (ACFP) gerecht werden.

Jedes Beispiel enthält eine Beschreibung des Anwendungsfalls und zeigt dann in JSON-Auflistungen die Lösung für die benutzerdefiniert konfigurierten Regeln an.

Note

Sie rufen JSON-Auflistungen wie die in diesen Beispielen dargestellten über den JSON-Download der Console-Web-ACL bzw. den JSON-Regel-Editor oder über den `getWebACL`-Betrieb in den APIs und der Befehlszeilenschnittstelle ab.

Themen

- [ACFP-Beispiel: Einfache Konfiguration](#)
- [ACFP-Beispiel: Benutzerdefinierte Antwort auf kompromittierte Anmeldeinformationen](#)
- [ACFP-Beispiel: Konfiguration der Reaktionsinspektion](#)

ACFP-Beispiel: Einfache Konfiguration

Die folgende JSON-Liste zeigt ein Beispiel für eine Web-ACL mit einer verwalteten Regelgruppe zur Erstellung von AWS WAF Fraud Control-Konten zur Betrugsprävention (Fraud Control Account Creation Fraud Prevention, ACFP). Notieren Sie sich die zusätzlichen `CreationPath` `RegistrationPagePath` Konfigurationen sowie den Payload-Typ und die Informationen, die erforderlich sind, um neue Kontoinformationen in der Payload zu finden und diese zu verifizieren. Die Regelgruppe verwendet diese Informationen, um Ihre Anfragen zur Kontoerstellung zu überwachen und zu verwalten. Diese JSON-Datei enthält die automatisch generierten Einstellungen der Web-ACL, etwa den Namespace der Bezeichnung und die URL zur Anwendungsintegration der Web-ACL.

```
{
  "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/phonenummer"  
          }  
        ],  
        "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": "awsaf:111122223333:webacl:simpleACFP:"
}

```

ACFP-Beispiel: Benutzerdefinierte Antwort auf kompromittierte Anmeldeinformationen

Standardmäßig `AWSManagedRulesACFPRuleSet` behandelt die Überprüfung der Anmeldeinformationen, die von der Regelgruppe durchgeführt wird, kompromittierte Anmeldeinformationen, indem sie die Anfrage kennzeichnet und blockiert. Weitere Informationen zur Regelgruppe und zum Regelverhalten finden Sie unter [AWS WAF Regelgruppe Betrugsprävention \(ACFP\) zur Kontoerstellung bei der Betrugsbekämpfung](#).

Um den Benutzer darüber zu informieren, dass die von ihm angegebenen Kontoanmeldeinformationen kompromittiert wurden, können Sie wie folgt vorgehen:

- **SignalCredentialCompromised** Regel überschreiben auf Count — Dadurch zählt und kennzeichnet die Regel nur übereinstimmende Anfragen.

- Fügen Sie eine Label-Abgleichsregel mit benutzerdefinierter Behandlung hinzu — Konfigurieren Sie diese Regel so, dass sie mit dem ACFP-Label übereinstimmt und Ihre benutzerdefinierte Behandlung durchführt.

Die folgenden Web-ACL-Listen zeigen die von ACFP verwaltete Regelgruppe aus dem vorherigen Beispiel, wobei die `SignalCredentialCompromised` Regelaktion überschrieben wurde, sodass sie zählt. Wenn diese Regelgruppe bei dieser Konfiguration eine Webanfrage auswertet, die kompromittierte Anmeldeinformationen verwendet, kennzeichnet sie die Anfrage, blockiert sie jedoch nicht.

Darüber hinaus hat die Web-ACL jetzt eine benutzerdefinierte Antwort mit dem Namen `aws-waf-credential-compromised` und eine neue Regel mit dem Namen.

`AccountSignupCompromisedCredentialsHandling` Bei der Regelpriorität handelt es sich um eine höhere numerische Einstellung als bei der Regelgruppe, sodass sie bei der Web-ACL-Evaluierung hinter der Regelgruppe ausgeführt wird. Die neue Regel gleicht alle Anfragen ab, die das Label „Kompromittierte Anmeldeinformationen“ der Regelgruppe aufweisen. Wenn die Regel eine Übereinstimmung findet, wendet sie die Block Aktion auf die Anfrage mit dem benutzerdefinierten Antworttext an. Der benutzerdefinierte Antworttext informiert den Endbenutzer darüber, dass seine Anmeldeinformationen kompromittiert wurden, und schlägt eine zu ergreifende Maßnahme vor.

```
{
  "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/phonenummer"
    }
  ],
  "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": "aws:waf: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": "aws-waf: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\"}"
    }
}
}
}

```

ACFP-Beispiel: Konfiguration der Reaktionsinspektion

Die folgende JSON-Liste zeigt ein Beispiel für eine Web-ACL mit einer verwalteten Regelgruppe zur Erstellung von AWS WAF Fraud Control-Konten zur Betrugsbekämpfung (Fraud Control Account Creation Fraud Prevention, Betrugsprävention), die für die Überprüfung von Antworten konfiguriert ist. Beachten Sie die Konfiguration der Antwortprüfung, in der Erfolgs- und Antwortstatuscodes angegeben sind. Sie können Erfolgs- und Antworteinstellungen auch auf der Grundlage von JSON-Übereinstimmungen in Header, Body und Body konfigurieren. Diese JSON-Datei enthält die automatisch generierten Einstellungen der Web-ACL, etwa den Namespace der Bezeichnung und die URL zur Anwendungsintegration der Web-ACL.

Note

Die ATP-Antwortprüfung ist nur in Web-ACLs verfügbar, die CloudFront Distributionen schützen.

```
{
  "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/phonenummer"
                    }
                  ]
                }
              }
            }
          ]
        }
      }
    }
  ]
}
```

```
        "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": "aws-waf-111122223333:webacl:simpleACFP:"
}
```

AWS WAF Verhinderung von Kontoübernahmen bei der Betrugsbekämpfung (ATP)

Kontoübernahmen sind eine illegale Online-Aktivität, bei der sich ein Angreifer unbefugten Zugriff auf das Konto einer anderen Person verschafft. Der Angreifer kann dies auf verschiedene Weise tun, z. B. mit gestohlenen Anmeldeinformationen oder indem er das Passwort des Opfers durch eine Reihe von Versuchen errät. Wenn sich der Angreifer Zugang verschafft, kann er Geld, Informationen oder Dienste des Opfers stehlen. Der Angreifer könnte sich als das Opfer ausgeben, um Zugang zu anderen Konten zu erhalten, die dem Opfer gehören, oder um Zugang zu den Konten anderer Personen oder Organisationen zu erhalten. Außerdem könnten sie versuchen, das Passwort des Benutzers zu ändern, um das Opfer aus seinen eigenen Konten auszusperrern.

Sie können Versuche zur Kontoübernahme überwachen und kontrollieren, indem Sie die Funktion zur Verhinderung von Kontoübernahmen (AWS WAF Fraud Control Account Takeover Prevention, ATP) implementieren. AWS WAF bietet diese Funktion in den SDKs für die Regelgruppe „AWS Verwaltete Regeln“ `AWSManagedRulesATPRuleSet` und in den zugehörigen SDKs zur Anwendungsintegration an.

Die von ATP verwaltete Regelgruppe kennzeichnet und verwaltet Anfragen, die Teil böswilliger Kontoübernahmeversuche sein könnten. Zu diesem Zweck untersucht die Regelgruppe Anmeldeversuche, die Clients an den Anmeldeendpunkt Ihrer Anwendung senden.

- Überprüfung von Anfragen — ATP bietet Ihnen Transparenz und Kontrolle über ungewöhnliche Anmeldeversuche und Anmeldeversuche, bei denen gestohlene Anmeldeinformationen verwendet werden, um Kontoübernahmen zu verhindern, die zu betrügerischen Aktivitäten führen könnten. ATP überprüft E-Mail- und Passwortkombinationen anhand seiner Datenbank mit gestohlenen Anmeldeinformationen, die regelmäßig aktualisiert wird, sobald neue durchgesickerte Anmeldeinformationen im Dark Web gefunden werden. ATP aggregiert Daten nach IP-Adresse und

Clientsitzung, um Clients zu erkennen und zu blockieren, die zu viele Anfragen verdächtiger Art senden.

- **Überprüfung der Antworten** — Bei CloudFront Verteilungen untersucht die ATP-Regelgruppe nicht nur eingehende Anmeldeanfragen, sondern auch die Antworten Ihrer Anwendung auf Anmeldeversuche, um Erfolgs- und Fehlschlagquoten nachzuverfolgen. Mithilfe dieser Informationen kann ATP vorübergehend Clientsitzungen oder IP-Adressen blockieren, bei denen zu viele Anmeldefehler aufgetreten sind. AWS WAF führt die Antwortprüfung asynchron durch, sodass die Latenz Ihres Webverkehrs dadurch nicht erhöht wird.

Note

Ihnen werden zusätzliche Gebühren berechnet, wenn Sie diese verwaltete Regelgruppe verwenden. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).

Note

Die ATP-Funktion ist für Amazon Cognito Cognito-Benutzerpools nicht verfügbar.

Themen


- [ATP-Komponenten](#)
- [Warum Sie die Anwendungsintegrations-SDKs mit ATP verwenden sollten](#)
- [Hinzufügen der von ATP verwalteten Regelgruppe zu Ihrer Web-ACL](#)
- [Testen und Bereitstellen von ATP](#)
- [AWS WAF Beispiele zur Verhinderung von Kontoübernahmen \(ATP\) bei der Betrugsbekämpfung](#)

ATP-Komponenten

Die wichtigsten Komponenten von AWS WAF Fraud Control Account Takeover Prevention (ATP) sind die folgenden:

- **AWSManagedRulesATPRuleSet**— Die Regeln in dieser Regelgruppe „AWS Verwaltete Regeln“ erkennen, kennzeichnen und behandeln verschiedene Arten von Kontoübernahmeaktivitäten. Die Regelgruppe untersucht POST HTTP-Webanfragen, die Clients an den angegebenen

Anmeldeendpunkt senden. Bei geschützten CloudFront Verteilungen überprüft die Regelgruppe auch die Antworten, die die Verteilung auf diese Anfragen zurücksendet. Eine Liste der Regeln der Regelgruppe finden Sie unter [AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen \(ATP\) zur Betrugsbekämpfung](#). Sie nehmen diese Regelgruppe in Ihre Web-ACL auf, indem Sie eine Referenzanweisung für die verwaltete Regelgruppe verwenden. Informationen zur Verwendung dieser Regelgruppe finden Sie unter [Hinzufügen der von ATP verwalteten Regelgruppe zu Ihrer Web-ACL](#).

 Note

Wenn Sie diese verwaltete Regelgruppe verwenden, werden Ihnen zusätzliche Gebühren berechnet. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).

- Details zur Anmeldeseite Ihrer Anwendung – Sie müssen Informationen über Ihre Anmeldeseite angeben, wenn Sie der Web-ACL die `AWSManagedRulesATPRuleSet`-Regelgruppe hinzufügen. Auf diese Weise kann die Regelgruppe den Umfang der Anfragen, die sie überprüft, einschränken und die Verwendung von Anmeldeinformationen in Webanfragen ordnungsgemäß überprüfen. Die ATP-Regelgruppe arbeitet mit Benutzernamen im E-Mail-Format. Weitere Informationen finden Sie unter [Hinzufügen der von ATP verwalteten Regelgruppe zu Ihrer Web-ACL](#).
- Bei geschützten CloudFront Distributionen: Details darüber, wie Ihre Anwendung auf Anmeldeversuche reagiert — Sie geben Details zu den Antworten Ihrer Anwendung auf Anmeldeversuche an, und die Regelgruppe verfolgt und verwaltet Clients, die zu viele fehlgeschlagene Anmeldeversuche senden. Informationen zur Konfiguration dieser Option finden Sie unter [Hinzufügen der von ATP verwalteten Regelgruppe zu Ihrer Web-ACL](#).
- JavaScript und SDKs für die Integration mobiler Anwendungen — Implementieren Sie die SDKs AWS WAF JavaScript und die mobilen SDKs zusammen mit Ihrer ATP-Implementierung, um alle Funktionen zu nutzen, die die Regelgruppe bietet. Viele der ATP-Regeln verwenden die von den SDKs bereitgestellten Informationen für die Client-Überprüfung auf Sitzungsebene und die Aggregation von Verhalten, die erforderlich sind, um legitimen Client-Verkehr von Bot-Verkehr zu trennen. Weitere Informationen zu den SDKs finden Sie unter [AWS WAF Integration von Client-Anwendungen](#).

Sie können Ihre ATP-Implementierung mit den folgenden Funktionen kombinieren, um Ihre Schutzmaßnahmen zu überwachen, zu optimieren und anzupassen.

- Protokollierung und Metriken — Sie können Ihren Datenverkehr überwachen und verstehen, wie sich die von ATP verwaltete Regelgruppe darauf auswirkt, indem Sie Logs und CloudWatch

Amazon-Metriken für Ihre Web-ACL konfigurieren und aktivieren. Die Labels, die Ihren Webanfragen `AWSManagedRulesATPRuleSet` hinzugefügt werden, sind in den Protokollen und in den CloudWatch Amazon-Metriken enthalten. Informationen zu Protokollierung und Metriken finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#) und [Überwachung mit Amazon CloudWatch](#).

Abhängig von Ihren Anforderungen und dem Datenverkehr, den Sie beobachten, möchten Sie Ihre `AWSManagedRulesATPRuleSet`-Implementierung möglicherweise anpassen. Beispielsweise möchten Sie möglicherweise einen Teil des Datenverkehrs von der ATP-Bewertung ausschließen oder die Art und Weise ändern, wie das Unternehmen mit einigen der von ihm identifizierten Kontoübernahmeversuche umgeht, indem Sie AWS WAF Funktionen wie Scopedown-Aussagen oder Regeln für den Label-Abgleich verwenden.

- Bezeichnungen und Regeln zum Abgleich von Bezeichnungen – Für jede der Regeln in `AWSManagedRulesATPRuleSet` können Sie das Blockierverhalten auf „Zählen“ umstellen und dann mit den Bezeichnungen abgleichen, die durch die Regeln hinzugefügt wurden. Verwenden Sie diesen Ansatz, um anzupassen, wie Sie mit Webanfragen umgehen, die von der ATP-verwalteten Regelgruppe identifiziert werden. Weitere Informationen zur Bezeichnung und zur Verwendung von Anweisungen zum Abgleich von Bezeichnungen finden Sie unter [Regelanweisung für Bezeichnungsübereinstimmung](#) und [AWS WAF Labels auf Webanfragen](#).
- Benutzerdefinierte Anforderungen und Antworten – Sie können den Anforderungen, die Sie zulassen, benutzerdefinierte Header hinzufügen, und Sie können für blockierte Anforderungen benutzerdefinierte Antworten senden. Dazu kombinieren Sie den Bezeichnungsabgleich mit den AWS WAF -Funktionen für benutzerdefinierte Anforderungen und Antworten. Weitere Informationen zum Anpassen von Anforderungen und Antworten finden Sie unter [Benutzerdefinierte Webanforderungen und Antworten in AWS WAF](#).

Warum Sie die Anwendungsintegrations-SDKs mit ATP verwenden sollten

Die von ATP verwaltete Regelgruppe benötigt die Challenge-Token, die von den Anwendungsintegrations-SDKs generiert werden. Die Token ermöglichen den vollständigen Schutz, den die Regelgruppe bietet.

Wir empfehlen dringend, die Anwendungsintegrations-SDKs zu implementieren, um die ATP-Regelgruppe am effektivsten nutzen zu können. Das Challenge-Skript muss vor der ATP-Regelgruppe ausgeführt werden, damit die Regelgruppe von den Tokens, die das Skript erhält, profitieren kann. Dies geschieht automatisch mit den SDKs für die Anwendungsintegration. Wenn Sie die SDKs nicht verwenden können, können Sie Ihre Web-ACL alternativ so konfigurieren, dass sie die CAPTCHA Regelaktion Challenge oder für alle Anfragen ausführt, die von der ATP-Regelgruppe

geprüft werden. Für die Verwendung der CAPTCHA Regelaktion Challenge oder können zusätzliche Gebühren anfallen. Details zu den Preisen finden Sie unter [AWS WAF -Preise](#).

Funktionen der ATP-Regelgruppe, für die kein Token erforderlich ist

Wenn Webanfragen kein Token haben, kann die von ATP verwaltete Regelgruppe die folgenden Arten von Datenverkehr blockieren:

- Einzelne IP-Adressen, die viele Anmeldeanfragen stellen.
- Einzelne IP-Adressen, die in kurzer Zeit viele fehlgeschlagene Anmeldeanfragen stellen.
- Anmeldeversuche mit Passwort-Traversal, wobei derselbe Benutzername verwendet wird, aber Passwörter geändert werden.

Funktionen der ATP-Regelgruppe, für die ein Token erforderlich ist

Die im Challenge-Token enthaltenen Informationen erweitern die Funktionen der Regelgruppe und die allgemeine Sicherheit Ihrer Client-Anwendung.

Das Token stellt bei jeder Webanforderung Client-Informationen bereit, die es der ATP-Regelgruppe ermöglichen, legitime Clientsitzungen von schlecht funktionierenden Clientsitzungen zu trennen, selbst wenn beide von einer einzigen IP-Adresse stammen. Die Regelgruppe verwendet die Informationen in den Tokens, um das Verhalten von Clientsitzungsanfragen zu aggregieren und so die Erkennung und Abwehr zu optimieren.

Wenn das Token in Webanfragen verfügbar ist, kann die ATP-Regelgruppe die folgenden zusätzlichen Kategorien von Clients auf Sitzungsebene erkennen und blockieren:

- Clientsitzungen, bei denen die automatische Abfrage, die von den SDKs verwaltet wird, nicht ausgeführt werden kann.
- Clientsitzungen, die Benutzernamen oder Passwörter durchlaufen. Dies wird auch als Credential Stuffing bezeichnet.
- Clientsitzungen, bei denen wiederholt gestohlene Anmeldeinformationen für die Anmeldung verwendet werden.
- Clientsitzungen, bei denen lange versucht wird, sich anzumelden.
- Kundensitzungen, die viele Anmeldeanfragen stellen. Die ATP-Regelgruppe bietet eine bessere Client-Isolierung als die AWS WAF ratenbasierte Regel, die Clients anhand ihrer IP-Adresse blockieren kann. Die ATP-Regelgruppe verwendet auch einen niedrigeren Schwellenwert.

- Client-Sitzungen, die in kurzer Zeit viele fehlgeschlagene Anmeldeanfragen stellen. Diese Funktion ist für geschützte CloudFront Amazon-Distributionen verfügbar.

Weitere Informationen zu den Funktionen von Regelgruppen finden Sie unter [AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen \(ATP\) zur Betrugsbekämpfung](#).

Informationen zu den SDKs finden Sie unter [AWS WAF Integration von Client-Anwendungen](#).

Informationen zu AWS WAF Tokens finden Sie unter [AWS WAF Webanforderungstoken](#).

Informationen zu den Regelaktionen finden Sie unter [CAPTCHA und Challenge in AWS WAF](#).

Hinzufügen der von ATP verwalteten Regelgruppe zu Ihrer Web-ACL

Um die von ATP verwaltete Regelgruppe so zu konfigurieren, dass sie Kontoübernahmeaktivitäten in Ihrem Web-Traffic erkennt, geben Sie Informationen darüber an, wie Clients Anmeldeanfragen an Ihre Anwendung senden. Für geschützte CloudFront Amazon-Distributionen geben Sie auch Informationen darüber an, wie Ihre Anwendung auf Anmeldeanfragen reagiert. Diese Konfiguration gilt zusätzlich zur normalen Konfiguration für eine verwaltete Regelgruppe.

Eine Beschreibung der Regelgruppe und eine Liste der Regeln finden Sie unter [AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen \(ATP\) zur Betrugsbekämpfung](#).

Note

Die ATP-Datenbank mit gestohlenen Anmeldeinformationen enthält nur Benutzernamen im E-Mail-Format.


Diese Anleitung richtet sich an Benutzer, die im Allgemeinen wissen, wie man Web-ACLs, Regeln und Regelgruppen für AWS WAF erstellt und verwaltet. Diese Themen werden in früheren Abschnitten dieses Handbuchs behandelt. Grundlegende Informationen zum Hinzufügen einer verwalteten Regelgruppe zu einer Web-ACL finden Sie unter [Hinzufügen einer verwalteten Regelgruppe zu einer Web-ACL über die Konsole](#).

Folgen Sie den bewährten Methoden

Verwenden Sie die ATP-Regelgruppe gemäß den bewährten Methoden unter [Bewährte Methoden für intelligente Bedrohungsabwehr](#).

So verwenden Sie die Regelgruppe **AWSManagedRulesATPRuleSet** in einer Web-ACL

1. Fügen Sie die AWS verwaltete Regelgruppe **AWSManagedRulesATPRuleSet** zu Ihrer Web-ACL hinzu und bearbeiten Sie die Regelgruppeneinstellungen vor dem Speichern.


 Note

Ihnen werden zusätzliche Gebühren berechnet, wenn Sie diese verwaltete Regelgruppe verwenden. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).

2. Geben Sie im Bereich Regelgruppenkonfiguration die Informationen ein, die die ATP-Regelgruppe zur Prüfung von Anmeldeanfragen verwendet.
 - a. Aktivieren Sie diese Option für Reguläre Ausdrücke in Pfaden verwenden, wenn Sie einen Abgleich mit regulären Ausdrücken für die Pfadspezifikationen Ihrer Anmeldeseite durchführen möchten AWS WAF .

AWS WAF unterstützt `libpcre` mit einigen Ausnahmen die von der PCRE-Bibliothek verwendete Mustersyntax. Die Bibliothek ist unter [PCRE - Perl Compatible Regular Expressions](#) (Perl-kompatible reguläre Ausdrücke) dokumentiert. Hinweise zur AWS WAF Unterstützung finden Sie unter [Musterabgleich mit regulären Ausdrücken in AWS WAF](#).

- b. Geben Sie unter Anmeldepfad den Pfad des Anmeldeendpunkts für Ihre Anwendung an. Die Regelgruppe untersucht nur HTTP-POST-Webanforderungen an den von Ihnen angegebenen Anmelde-Endpunkt.

 Note

Beim Abgleich für Endpunkte wird nicht zwischen Groß- und Kleinschreibung unterschieden. Regex-Spezifikationen dürfen das Flag nicht enthalten (`?-i`), wodurch der Abgleich ohne Berücksichtigung der Groß- und Kleinschreibung deaktiviert wird. Zeichenkettenspezifikationen müssen mit einem Schrägstrich beginnen. /

Für die URL könnten Sie `https://example.com/web/login` beispielsweise die Pfadangabe `/web/login` für die Zeichenfolge angeben. Anmeldepfade, die mit dem von Ihnen angegebenen Pfad beginnen, werden als übereinstimmend betrachtet. `/web/login` entspricht beispielsweise den Anmeldepfaden `/web/login/web/login/,/web/`

loginPage, und/web/login/thisPage, entspricht aber nicht dem Anmeldepfad /home/web/login oder/website/login.

- c. Geben Sie für die Überprüfung von Anfragen an, wie Ihre Anwendung Anmeldeversuche akzeptiert, indem Sie den Payload-Typ der Anfrage und die Namen der Felder im Anfragetext angeben, in denen der Benutzername und das Passwort angegeben werden. Ihre Angabe der Feldnamen hängt vom Payload-Typ ab.
- JSON-Nutzdatentyp — Geben Sie die Feldnamen in der JSON-Zeigersyntax an. Informationen zur JSON-Pointer-Syntax finden Sie in der Dokumentation [JavaScriptObject Notation \(JSON\) Pointer der Internet Engineering Task Force \(IETF\)](#).


Für die folgende Beispiel-JSON-Nutzlast lautet die Feldspezifikation für den Benutzernamen /login/username und die Feldspezifikation für das Passwort. /login/password

```
{
  "login": {
    "username": "THE_USERNAME",
    "password": "THE_PASSWORD"
  }
}
```

- Payload-Typ FORM_ENCODED — Verwenden Sie die HTML-Formularnamen.

Für ein HTML-Formular mit Eingabeelementen mit dem Namen username1 und lautet username1 die Feldspezifikation für den Benutzernamen und password1 die Feldspezifikation für das Passwort. password1

- d. Wenn Sie CloudFront Amazon-Distributionen schützen, geben Sie unter Antwortprüfung an, wie Ihre Anwendung bei den Antworten auf Anmeldeversuche auf Erfolg oder Misserfolg hinweist.

 Note

Die ATP-Antwortprüfung ist nur in Web-ACLs verfügbar, die Distributionen schützen CloudFront .

Geben Sie eine einzelne Komponente in der Anmeldeantwort an, die ATP überprüfen soll. AWS WAF kann bei den Komponententypen Body und JSON die ersten 65.536 Byte (64 KB) der Komponente untersuchen.

Geben Sie Ihre Prüfkriterien für den Komponententyp an, wie in der Schnittstelle angegeben. Sie müssen sowohl Erfolgs- als auch Fehlschlagskriterien angeben, nach denen die Komponente geprüft werden soll.

Nehmen wir zum Beispiel an, Ihre Anwendung gibt den Status eines Anmeldeversuchs im Statuscode der Antwort an und verwendet ihn 200 OK für Erfolg 401 Unauthorized und/oder 403 Forbidden für Fehlschlag. Sie würden den Komponententyp der Antwortprüfung auf Statuscode setzen und dann in das Textfeld Erfolg 200 und im Textfeld Fehler den Text in 401 der ersten Zeile und in 403 der zweiten Zeile eingeben.

Die ATP-Regelgruppe zählt nur Antworten, die Ihren Erfolgs- oder Fehlschlagprüfungskriterien entsprechen. Die Regelgruppenregeln gelten für Clients, bei denen die Anzahl der gezählten Antworten zu hoch ist. Stellen Sie sicher, dass Sie vollständige Informationen zu erfolgreichen und fehlgeschlagenen Anmeldeversuchen angeben, damit sich die Regelgruppenregeln korrekt verhalten.

Die Regeln zur Prüfung von Login-Antworten finden Sie `VolumetricSessionFailedLoginResponseHigh` in der Regelliste unter [AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen \(ATP\) zur Betrugsbekämpfung](#).
`VolumetricIpFailedLoginResponseHigh`

3. Geben Sie jede zusätzliche Konfiguration an, die für die Regelgruppe benötigt wird.

Sie können den Umfang der Anforderungen, die von der Regelgruppe geprüft werden, weiter eingrenzen, indem Sie der Anweisung für die verwaltete Regelgruppe eine Eingrenzungsanweisung hinzufügen. So können Sie beispielsweise nur Anforderungen mit einem bestimmten Abfrageargument oder Cookie prüfen. Die Regelgruppe untersucht nur POST HTTP-Anfragen an Ihren angegebenen Anmeldeendpunkt, die den Kriterien in Ihrer Scope-down-Erklärung entsprechen. Informationen zu Eingrenzungsanweisungen finden Sie unter [Eingrenzungsanweisungen](#).

4. Speichern Sie Ihre Änderungen an der Web-ACL.

Bevor Sie Ihre ATP-Implementierung für den Produktionsdatenverkehr bereitstellen, sollten Sie sie in einer Staging- oder Testumgebung testen und optimieren, bis Sie mit den möglichen Auswirkungen auf Ihren Datenverkehr vertraut sind. Testen und optimieren Sie dann die Regeln im Zählmodus mit Ihrem Produktionsdatenverkehr, bevor Sie sie aktivieren. Weitere Informationen finden Sie im folgenden Abschnitt.

Testen und Bereitstellen von ATP

Dieser Abschnitt enthält allgemeine Anleitungen zur Konfiguration und zum Testen einer ATP-Implementierung (AWS WAF Fraud Control Account Takeover Prevention) für Ihre Website. Für welche Schritte Sie sich im Einzelnen entscheiden, hängt von Ihren Anforderungen, Ihren Ressourcen und den bei Ihnen eingehenden Webanforderungen ab.

Diese Informationen ergänzen die allgemeinen Informationen zum Testen und Optimieren, die Sie unter finden [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

Note

AWS Verwaltete Regeln wurden entwickelt, um Sie vor gängigen Internet-Bedrohungen zu schützen. Wenn sie gemäß der Dokumentation verwendet werden, bieten Regelgruppen mit AWS verwalteten Regeln eine weitere Sicherheitsebene für Ihre Anwendungen. Regelgruppen mit AWS verwalteten Regeln sind jedoch nicht als Ersatz für Ihre Sicherheitsaufgaben gedacht, die durch die von Ihnen ausgewählten AWS Ressourcen bestimmt werden. Anhand des [Modells der gemeinsamen Verantwortung](#) können Sie sicherstellen, dass Ihre Ressourcen ordnungsgemäß geschützt AWS sind.

Risiken rund um Produktionsdatenverkehr

Bevor Sie Ihre ATP-Implementierung für den Produktionsdatenverkehr bereitstellen, sollten Sie sie in einer Staging- oder Testumgebung testen und optimieren, bis Sie mit den möglichen Auswirkungen auf Ihren Datenverkehr vertraut sind. Testen und optimieren Sie dann die Regeln im Zählmodus mit Ihrem Produktionsdatenverkehr, bevor Sie sie aktivieren.

AWS WAF stellt Testanmeldedaten bereit, mit denen Sie Ihre ATP-Konfiguration überprüfen können. Im Folgenden konfigurieren Sie eine Test-Web-ACL, um die verwaltete ATP-Regelgruppe zu verwenden, konfigurieren eine Regel, um die von der Regelgruppe hinzugefügte Bezeichnung zu


erfassen, und führen dann einen Anmeldeversuch mit diesen Testanmeldeinformationen durch. Sie überprüfen, ob Ihre Web-ACL den Versuch ordnungsgemäß verwaltet hat, indem Sie die CloudWatch Amazon-Metriken für den Anmeldeversuch überprüfen.

Diese Anleitung richtet sich an Benutzer, die im Allgemeinen wissen, wie man Web-ACLs, Regeln und Regelgruppen für AWS WAF erstellt und verwaltet. Diese Themen werden in früheren Abschnitten dieses Handbuchs behandelt.

Um eine ATP-Implementierung (AWS WAF Fraud Control Account Takeover Prevention) zu konfigurieren und zu testen

Führen Sie diese Schritte zuerst in einer Testumgebung und dann in der Produktion aus.

1. Fügen Sie die verwaltete Regelgruppe zur Verhinderung von Kontoübernahmen (AWS WAF Fraud Control Account Takeover Prevention, ATP) im Zählmodus hinzu

 Note

Ihnen werden zusätzliche Gebühren berechnet, wenn Sie diese verwaltete Regelgruppe verwenden. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).

Fügen Sie die Regelgruppe `AWSManagedRulesATPRuleSet` „AWS Verwaltete Regeln“ einer neuen oder vorhandenen Web-ACL hinzu und konfigurieren Sie sie so, dass sie das aktuelle Verhalten der Web-ACL nicht verändert. Weitere Informationen zu den Regeln und Bezeichnungen für diese Regelgruppe finden Sie unter [AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen \(ATP\) zur Betrugsbekämpfung](#).

- Wenn Sie die verwaltete Regelgruppe hinzufügen, bearbeiten Sie sie und gehen Sie wie folgt vor:
 - Geben Sie im Bereich Rule group configuration (Regelgruppenkonfiguration) die Details der Anmeldeseite Ihrer Anwendung an. Die ATP-Regelgruppe verwendet diese Informationen, um Anmeldeaktivitäten zu überwachen. Weitere Informationen finden Sie unter [Hinzufügen der von ATP verwalteten Regelgruppe zu Ihrer Web-ACL](#).
 - Öffnen Sie im Bereich Regeln die Dropdownliste Alle Regelaktionen außer Kraft setzen und wählen Sie Count. Mit dieser Konfiguration wertet AWS WAF Anforderungen nach allen Regeln in der Regelgruppe aus und zählt nur die daraus resultierenden Übereinstimmungen.

Gleichzeitig werden weiterhin Beschriftungen zu Anforderungen hinzugefügt. Weitere Informationen finden Sie unter [Regelaktionen in einer Regelgruppe überschreiben](#).

Mit dieser Außerkraftsetzung können Sie die potenziellen Auswirkungen der von ATP verwalteten Regeln überwachen und entscheiden, ob Sie Ausnahmen hinzufügen möchten, z. B. Ausnahmen für interne Anwendungsfälle.

- Positionieren Sie die Regelgruppe so, dass sie nach Ihren vorhandenen Regeln in der Web-ACL ausgewertet wird, mit einer Prioritätseinstellung, die numerisch höher ist als alle Regeln oder Regelgruppen, die Sie bereits verwenden. Weitere Informationen finden Sie unter [Reihenfolge der Verarbeitung von Regeln und Regelgruppen in einer Web-ACL](#).

Auf diese Weise wird Ihre derzeitige Handhabung des Datenverkehrs nicht gestört. Wenn Sie beispielsweise Regeln haben, die böartigen Datenverkehr wie SQL-Injections oder Cross-Site-Scripting erkennen, erkennen und protokollieren sie diese Probleme weiterhin. Wenn Sie über Regeln verfügen, die bekannten nicht böswilligen Datenverkehr zulassen, lassen diese derartigen Datenverkehr weiterhin zu, ohne dass er von der durch ATP verwalteten Regelgruppe blockiert wird. Möglicherweise entscheiden Sie sich, die Verarbeitungsreihenfolge während Ihrer Test- und Optimierungsaktivitäten anzupassen.

2. Aktivieren von Sampling, Protokollierung und Metriken für die Web-ACL

Konfigurieren Sie bei Bedarf die Protokollierung für die Web-ACL und aktivieren Sie Sampling und CloudWatch Amazon-Metriken. Sie können diese Sichtbarkeitstools verwenden, um die Interaktion der von ATP verwalteten Regelgruppe mit Ihrem Datenverkehr zu überwachen.

- Weitere Informationen zum Konfigurieren und Verwenden der Protokollierung finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).
- Informationen zu CloudWatch Amazon-Metriken finden Sie unter [Überwachung mit Amazon CloudWatch](#).
- Informationen zum Sampling von Webanforderungen finden Sie unter [Anzeigen einer Stichprobe von Webanforderungen](#).

3. Zuordnen der Web-ACL zu einer Ressource

Wenn die Web-ACL noch keiner Testressource zugeordnet ist, ordnen Sie sie zu. Weitere Informationen finden Sie unter [Zuordnen oder Aufheben der Zuordnung einer Web-ACL zu einer Ressource AWS](#).

4. Überwachen des Datenverkehrs und der ATP-Regelübereinstimmungen

Stellen Sie sicher, dass Ihr normaler Datenverkehr fließt und dass durch die Regeln der durch ATP verwalteten Regelgruppe Bezeichnungen zu übereinstimmenden Webanforderungen hinzugefügt werden. Sie können die Labels in den Protokollen und die ATP- und Label-Metriken in den CloudWatch Amazon-Metriken sehen. In den Protokollen werden die Regeln, die Sie zur Zählung in der Regelgruppe außer Kraft gesetzt haben, im Feld mit auf Anzahl `action` gesetzt und `ruleGroupList` mit der `overriddenAction` Angabe der konfigurierten Regelaktion angezeigt, die Sie überschrieben haben.

5. Testen der Regelgruppenfunktionen zur Überprüfung von Anmeldeinformationen

Führen Sie einen Anmeldeversuch durch, bei dem Sie kompromittierte Anmeldeinformationen testen, und überprüfen Sie, ob die Regelgruppe wie erwartet mit ihnen übereinstimmt.

a. Melden Sie sich mit dem folgenden AWS WAF Test-Anmeldeinformationspaar auf der Anmeldeseite Ihrer geschützten Ressource an:

- Benutzer: `WAF_TEST_CREDENTIAL@wafexample.com`
- Passwort: `WAF_TEST_CREDENTIAL_PASSWORD`

Diese Testanmeldedaten werden als kompromittierte Anmeldeinformationen eingestuft, und die von ATP verwaltete Regelgruppe fügt der Anmeldeanforderung die `aws:waf:managed:aws:atp:signal:credential_compromised` Bezeichnung hinzu, die Sie in den Protokollen sehen können.

b. Suchen Sie in Ihren Web-ACL-Protokollen nach der `aws:waf:managed:aws:atp:signal:credential_compromised` Bezeichnung im `labels` Feld in den Protokolleinträgen für Ihre Webanfragen zur Testanmeldung. Weitere Informationen zur Protokollierung finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).

Nachdem Sie sich vergewissert haben, dass die Regelgruppe kompromittierte Anmeldeinformationen wie erwartet erfasst, können Sie Maßnahmen ergreifen, um die Implementierung für Ihre geschützte Ressource nach Bedarf zu konfigurieren.

6. Testen Sie bei CloudFront Verteilungen die Verwaltung von Anmeldefehlern durch die Regelgruppe

- a. Führen Sie für jedes Fehlerreaktionskriterium, das Sie für die ATP-Regelgruppe konfiguriert haben, einen Test durch. Warten Sie zwischen den Tests mindestens 10 Minuten.

Um ein einzelnes Fehlschlagkriterium zu testen, identifizieren Sie in der Antwort einen Anmeldeversuch, der mit diesen Kriterien fehlschlagen wird. Führen Sie dann von einer einzigen Client-IP-Adresse aus mindestens 10 fehlgeschlagene Anmeldeversuche in weniger als 10 Minuten durch.

Nach den ersten 6 Fehlschlägen sollte die Regel für volumetrische fehlgeschlagene Anmeldeversuche mit den übrigen Versuchen vergleichen und diese kennzeichnen und zählen. Aufgrund der Latenz kann es sein, dass die Regel die ersten ein oder zwei nicht berücksichtigt.

- b. Suchen Sie in Ihren Web-ACL-Protokollen nach der `aws:waf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high` Bezeichnung im `labels` Feld in den Protokolleinträgen für Ihre Webanfragen zur Testanmeldung. Weitere Informationen zur Protokollierung finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).

Diese Tests überprüfen, ob Ihre Fehlerkriterien Ihren Antworten entsprechen, indem geprüft wird, ob die Anzahl der fehlgeschlagenen Anmeldungen die Schwellenwerte für die Regel überschreitet. `VolumetricIpFailedLoginResponseHigh` Wenn Sie nach Erreichen der Schwellenwerte weiterhin Anmeldeanfragen von derselben IP-Adresse senden, gilt die Regel weiterhin, bis die Ausfallrate unter den Schwellenwert fällt. Solange die Schwellenwerte überschritten werden, berücksichtigt die Regel sowohl erfolgreiche als auch fehlgeschlagene Anmeldungen von der IP-Adresse aus.

7. Anpassen der Bearbeitung von ATP-Webanforderungen

Fügen Sie bei Bedarf Ihre eigenen Regeln hinzu, die Anforderungen explizit zulassen oder blockieren. Dadurch ändern Sie, wie ATP-Regeln andernfalls damit umgehen würden.

Sie können beispielsweise ATP-Bezeichnungen verwenden, um Anforderungen zuzulassen oder zu blockieren oder die Anforderungsbehandlung anzupassen. Sie können nach der durch ATP verwalteten Regelgruppe eine Übereinstimmungsregel für die Bezeichnung hinzufügen, um entsprechend bezeichnete Anforderungen für die Behandlung zu filtern, die Sie anwenden möchten. Behalten Sie nach dem Testen die zugehörigen ATP-Regeln im Zählmodus und die Entscheidungen zur Anforderungsbehandlung in Ihrer benutzerdefinierten Regel. Ein Beispiel

finden Sie unter [ATP-Beispiel: Benutzerdefinierte Behandlung fehlender und kompromittierter Anmeldeinformationen](#).

8. Entfernen Sie Ihre Testregeln und aktivieren Sie die Einstellungen für verwaltete ATP-Regelgruppen

Abhängig von Ihrer Situation haben Sie möglicherweise entschieden, dass Sie einige ATP-Regeln im Zählmodus belassen möchten. Für die Regeln, die Sie wie in der Regelgruppe konfiguriert ausführen möchten, deaktivieren Sie den Zählmodus in der Web-ACL-Regelgruppenkonfiguration. Wenn Sie mit dem Testen fertig sind, können Sie auch Ihre Testlabel-Vergleichsregeln entfernen.

9. Überwachen und Anpassen

Damit Webanforderungen wie gewünscht bearbeitet werden, sollten Sie Ihren Datenverkehr genau überwachen, nachdem Sie die gewünschte ATP-Funktionalität aktiviert haben. Passen Sie das Verhalten nach Bedarf mit der Überschreibung der Regelzählung für die Regelgruppe und mit Ihren eigenen Regeln an.

Wenn Sie mit dem Testen Ihrer ATP-Regelgruppenimplementierung fertig sind, empfehlen wir Ihnen dringend, das AWS WAF JavaScript SDK in Ihre Browser-Anmeldeseite zu integrieren, falls Sie dies noch nicht getan haben, um die Erkennungsmöglichkeiten zu verbessern. AWS WAF bietet auch mobile SDKs zur Integration von iOS- und Android-Geräten. Weitere Informationen zum den Integrations-SDKs finden Sie unter [AWS WAF Integration von Client-Anwendungen](#). Informationen zu dieser Empfehlung finden Sie unter [Warum Sie die Anwendungsintegrations-SDKs mit ATP verwenden sollten](#).

AWS WAF Beispiele zur Verhinderung von Kontoübernahmen (ATP) bei der Betrugsbekämpfung

In diesem Abschnitt finden Sie Beispielkonfigurationen für häufige Anwendungsfälle für Implementierungen der Verhinderung der Kontoübernahme (ATP) zur Betrugskontrolle mit AWS WAF .

Jedes Beispiel enthält eine Beschreibung des Anwendungsfalls und zeigt dann in JSON-Auflistungen die Lösung für die benutzerdefiniert konfigurierten Regeln an.

Note

Sie rufen JSON-Auflistungen wie die in diesen Beispielen dargestellten über den JSON-Download der Console-Web-ACL bzw. den JSON-Regel-Editor oder über den `getWebACL`-Betrieb in den APIs und der Befehlszeilenschnittstelle ab.

Themen

- [ATP-Beispiel: Einfache Konfiguration](#)
- [ATP-Beispiel: Benutzerdefinierte Behandlung fehlender und kompromittierter Anmeldeinformationen](#)
- [ATP-Beispiel: Konfiguration der Reaktionsinspektion](#)

ATP-Beispiel: Einfache Konfiguration

Die folgende JSON-Liste zeigt ein Beispiel für eine Web-ACL mit einer von AWS WAF Fraud Control verwalteten Regelgruppe zur Verhinderung von Kontoübernahmen (Fraud Control Account Takeover Prevention, ATP). Beachten Sie die zusätzliche Konfiguration der Anmeldeseite, die der Regelgruppe die Informationen gibt, die sie zur Überwachung und Verwaltung Ihrer Anmeldeanfragen benötigt. Diese JSON-Datei enthält die automatisch generierten Einstellungen der Web-ACL, etwa den Namespace der Bezeichnung und die URL zur Anwendungsintegration der Web-ACL.

```
{
  "WebACL": {
    "LabelNamespace": "aws-waf: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.awsaf.com/9z87abce34ea/1234567a1b10/",
  "LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}

```

```
}
```

ATP-Beispiel: Benutzerdefinierte Behandlung fehlender und kompromittierter Anmeldeinformationen

Standardmäßig werden bei den Anmeldeüberprüfungen, die von der Regelgruppe `AWSManagedRulesATPRuleSet` durchgeführt werden, Webanforderungen wie folgt behandelt:

- Fehlende Anmeldeinformationen: Anforderung wird beschriftet und blockiert.
- Kompromittierte Anmeldeinformationen: Anforderung wird beschriftet, aber nicht blockiert oder gezählt.

Weitere Informationen zur Regelgruppe und zum Regelverhalten finden Sie unter [AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen \(ATP\) zur Betrugsbekämpfung](#).

Sie können eine benutzerdefinierte Behandlung für Webanforderungen mit fehlenden oder kompromittierten Anmeldeinformationen hinzufügen, indem Sie wie folgt vorgehen:

- **MissingCredential**Regel überschreiben bis Count — Diese Regelaktionsüberschreibung bewirkt, dass die Regel nur übereinstimmende Anfragen zählt und kennzeichnet.
- Fügen Sie eine Regel zur Zuordnung von Bezeichnungen mit benutzerdefinierter Behandlung hinzu — Konfigurieren Sie diese Regel so, dass sie mit beiden ATP-Bezeichnungen übereinstimmt und Ihre benutzerdefinierte Behandlung durchführt. Beispielsweise können Sie den Kunden auf Ihre Anmeldeseite umleiten.

Die folgende Regel zeigt die von ATP verwaltete Regelgruppe aus dem vorherigen Beispiel, wobei die `MissingCredential` Regelaktion überschrieben wurde, sodass sie zählt. Dadurch wendet die Regel ihre Bezeichnung auf übereinstimmende Anfragen an und zählt dann nur die Anfragen, anstatt sie zu blockieren.

```
"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": []
    }
  }
],

```

Wenn die Regelgruppe mit dieser Konfiguration eine Webanforderung mit fehlenden oder kompromittierten Anmeldeinformationen auswertet, beschriftet sie die Anforderung, blockiert sie aber nicht.

Die Priorität der folgenden Regel ist numerisch höher als die der vorherigen Regelgruppe. AWS WAF wertet Regeln in numerischer Reihenfolge aus, beginnend mit der niedrigsten Zahl, sodass diese


Regel erst nach der Regelgruppenauswertung ausgewertet wird. Die Regel ist so konfiguriert, dass sie mit einer der Bezeichnungen der Anmeldeinformationen übereinstimmt und bei entsprechenden Anfragen eine benutzerdefinierte Antwort sendet.

```
"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"
  }
}
```

ATP-Beispiel: Konfiguration der Reaktionsinspektion

Die folgende JSON-Liste zeigt ein Beispiel für eine Web-ACL mit einer von AWS WAF Fraud Control Account Takeover Prevention (ATP) verwalteten Regelgruppe, die so konfiguriert ist, dass sie die ursprünglichen Antworten überprüft. Beachten Sie die Konfiguration der Antwortprüfung, in der

Erfolgs- und Antwortstatuscodes angegeben sind. Sie können Erfolgs- und Antworteinstellungen auch auf der Grundlage von JSON-Übereinstimmungen in Header, Body und Body konfigurieren. Diese JSON-Datei enthält die automatisch generierten Einstellungen der Web-ACL, etwa den Namespace der Bezeichnung und die URL zur Anwendungsintegration der Web-ACL.

 Note

Die ATP-Antwortprüfung ist nur in Web-ACLs verfügbar, die CloudFront Distributionen schützen.

```
{
  "WebACL": {
    "LabelNamespace": "awsmaf: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.awsaf.com/9z87abce34ea/1234567a1b10/",
"LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}

```

AWS WAF Bot-Steuerung

Mit Bot Control können Sie Bots wie Scraper, Scanner, Crawler, Statusmonitore und Suchmaschinen auf einfache Weise überwachen, blockieren oder ihre Geschwindigkeit einschränken. Wenn Sie die gezielte Inspektionsebene der Regelgruppe verwenden, können Sie auch Bots herausfordern, die sich nicht selbst identifizieren, wodurch es für böartige Bots schwieriger und teurer wird, gegen Ihre Website vorzugehen. Sie können Ihre Anwendungen allein mit der verwalteten Regelgruppe Bot Control oder in Kombination mit anderen Regelgruppen für AWS verwaltete Regeln und Ihren eigenen benutzerdefinierten AWS WAF Regeln schützen.

Bot Control umfasst ein Konsolen-Dashboard, das anhand des Samplings von Webanforderungen anzeigt, wie viel von Ihrem aktuellen Datenverkehr von Bots stammt. Wenn Sie die verwaltete Bot-Control-Regelgruppe zu Ihrer Web-ACL hinzufügen, können Sie Maßnahmen gegen Bot-Datenverkehr ergreifen und erhalten detaillierte Echtzeitinformationen über den allgemeinen Bot-Datenverkehr, der auf Ihre Anwendungen zugreift.

Note

Wenn Sie diese verwaltete Regelgruppe verwenden, werden Ihnen zusätzliche Gebühren berechnet. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).

Die verwaltete Regelgruppe Bot Control bietet eine grundlegende, gemeinsame Schutzebene, die selbstidentifizierende Bots kennzeichnet, allgemein erwünschte Bots verifiziert und Bot-Signaturen mit hoher Vertrauenswürdigkeit erkennt. Dies gibt Ihnen die Möglichkeit, gängige Kategorien von Bot-Traffic zu überwachen und zu kontrollieren.

Die Regelgruppe Bot Control bietet außerdem eine gezielte Schutzstufe, die die Erkennung komplexer Bots, die sich nicht selbst identifizieren, ermöglicht. Gezielte Schutzmaßnahmen verwenden Erkennungstechniken wie Browserabfragen, Fingerabdrücke und Verhaltensheuristiken, um böartigen Bot-Traffic zu identifizieren. Darüber hinaus bieten gezielte Schutzmaßnahmen eine optionale automatisierte, maschinelle Lernanalyse der Besucherstatistiken auf Websites, um Aktivitäten im Zusammenhang mit Bots zu erkennen. Wenn Sie maschinelles Lernen aktivieren, AWS WAF verwendet es Statistiken über den Webseitenverkehr, wie Zeitstempel, Browsereigenschaften und zuvor besuchte URLs, um das maschinelle Lernmodell von Bot Control zu verbessern.

Weitere Informationen zur verwalteten Regelgruppe von Bot Control finden Sie unter [AWS WAF Regelgruppe „Bot-Kontrolle“](#).

Wenn eine Webanfrage anhand der von Bot Control verwalteten Regelgruppe AWS WAF bewertet wird, fügt die Regelgruppe Anfragen, die sie als bot-bezogen erkennt, Labels hinzu, z. B. die Bot-Kategorie und den Bot-Namen. Sie können diese Bezeichnungen in Ihren eigenen AWS WAF Regeln abgleichen, um die Handhabung anzupassen. Die Labels, die von der verwalteten Regelgruppe Bot Control generiert werden, sind in den CloudWatch Amazon-Metriken und Ihren Web-ACL-Protokollen enthalten.

Sie können AWS Firewall Manager AWS WAF Richtlinien auch verwenden, um die von Bot Control verwaltete Regelgruppe in Ihren Anwendungen in mehreren Konten bereitzustellen, die Teil Ihrer Organisation sind AWS Organizations.

Komponenten von Bot Control

Die Hauptkomponenten einer Bot-Control-Implementierung sind die folgenden:

- **AWSManagedRulesBotControlRuleSet**— Die von Bot Control verwaltete Regelgruppe, deren Regeln verschiedene Kategorien von Bots erkennen und behandeln. Diese Regelgruppe fügt den Webanforderungen, die sie als Bot-Datenverkehr erkennt, Bezeichnungen hinzu.

Note

Ihnen werden zusätzliche Gebühren berechnet, wenn Sie diese verwaltete Regelgruppe verwenden. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).

Die verwaltete Regelgruppe von Bot Control bietet zwei Schutzstufen, aus denen Sie wählen können:

- **Allgemein** — Erkennt eine Vielzahl von sich selbst identifizierenden Bots, z. B. Web-Scraping-Frameworks, Suchmaschinen und automatisierte Browser. Bot-Control-Schutzmaßnahmen auf dieser Ebene identifizieren häufig auftretende Bots mithilfe herkömmlicher Bot-Erkennungstechniken, wie z. B. der Analyse statischer Anforderungsdaten. Die Regeln kennzeichnen den Traffic dieser Bots und blockieren diejenigen, die sie nicht verifizieren können.
- **Gezielt** — Beinhaltet Schutzmaßnahmen auf allgemeiner Ebene und bietet eine gezielte Erkennung für ausgeklügelte Bots, die sich nicht selbst identifizieren. Gezielte Schutzmaßnahmen reduzieren Bot-Aktivitäten mithilfe einer Kombination aus Ratenbegrenzung und CAPTCHA sowie Browser-Herausforderungen im Hintergrund.

- **TGT_**— Regeln, die gezielten Schutz bieten, haben Namen, die mit **TGT_** beginnen. Alle gezielten Schutzmaßnahmen verwenden Erkennungstechniken wie Browserabfragen, Fingerabdrücke und Verhaltensheuristiken, um böartigen Bot-Traffic zu identifizieren.
- **TGT_ML_**— Gezielte Schutzregeln, die maschinelles Lernen verwenden, haben Namen, die mit **TGT_ML_** beginnen. Diese Regeln verwenden automatisierte, maschinelle Lernanalysen der Besucherstatistiken von Websites, um ungewöhnliches Verhalten zu erkennen, das auf verteilte, koordinierte Bot-Aktivitäten hindeutet. AWS WAF analysiert Statistiken über Ihren Website-Verkehr wie Zeitstempel, Browsereigenschaften und die zuvor besuchte URL, um das maschinelle Lernmodell von Bot Control zu verbessern. Funktionen für maschinelles Lernen sind standardmäßig aktiviert, Sie können sie jedoch in Ihrer Regelgruppenkonfiguration deaktivieren. Wenn maschinelles Lernen deaktiviert ist, werden diese Regeln von AWS WAF nicht ausgewertet.

Einzelheiten, einschließlich Informationen zu den Regeln der Regelgruppe, finden Sie unter [AWS WAF Regelgruppe „Bot-Kontrolle“](#).

Sie nehmen diese Regelgruppe mithilfe einer Referenzanweisung für verwaltete Regelgruppen in Ihre Web-ACL auf und geben die Inspektionsebene an, die Sie verwenden möchten. Für die Zielebene geben Sie auch an, ob maschinelles Lernen aktiviert werden soll. Weitere Informationen zum Hinzufügen dieser verwalteten Regelgruppe zu Ihrer Web-ACL finden Sie unter [Hinzufügen der von AWS WAF Bot Control verwalteten Regelgruppe zu Ihrer Web-ACL](#).

- **Bot-Control-Dashboard** – Das Bot-Überwachungs-Dashboard für Ihre Web-ACL, das über die Web-ACL-Registerkarte „Bot Control“ verfügbar ist. Verwenden Sie dieses Dashboard, um Ihren Datenverkehr zu überwachen und zu ermitteln, wie viel davon von den verschiedenen Arten von Bots stammt. Dies kann ein Ausgangspunkt für die Anpassung Ihres Bot-Managements sein, wie in diesem Thema beschrieben. Sie können es auch verwenden, um Ihre Änderungen zu überprüfen und die Aktivität verschiedener Bots und Bot-Kategorien zu überwachen.
- **JavaScript und SDKs zur Integration mobiler Anwendungen** — Sie sollten die SDKs von AWS WAF für JavaScript und die mobilen SDKs implementieren, wenn Sie die gezielte Schutzstufe der Bot Control-Regelgruppe verwenden. Die gezielten Regeln verwenden Informationen, die von den SDKs in den Client-Token bereitgestellt werden, um die Erkennung bössartiger Bots zu verbessern. Weitere Informationen zu den SDKs finden Sie unter [AWS WAF Integration von Client-Anwendungen](#).
- **Protokollierung und Metriken** — Sie können Ihren Bot-Traffic überwachen und verstehen, wie die von Bot Control verwaltete Regelgruppe Ihren Traffic bewertet und verarbeitet, indem Sie die Logs und CloudWatch Amazon-Metriken für Ihre Web-ACL untersuchen. Die Labels, die Bot Control

Ihren Webanfragen hinzufügt, sind in den Protokollen und in den CloudWatch Amazon-Metriken enthalten. Informationen zur Konfiguration und Verwendung von Protokollierung und Metriken finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#) und [Überwachung mit Amazon CloudWatch](#).

Abhängig von Ihren Anforderungen und dem Datenverkehr, den Sie beobachten, möchten Sie Ihre Bot-Control-Implementierung möglicherweise anpassen. Im Folgenden sind einige der am häufigsten verwendeten Optionen aufgeführt.

- **Scope-down-Aussagen** — Sie können einen Teil des Datenverkehrs von den Webanfragen ausschließen, die von der von Bot Control verwalteten Regelgruppe ausgewertet werden, indem Sie der Referenzanweisung für die verwaltete Regelgruppe von Bot Control eine Scopedown-Anweisung hinzufügen. Jede verschachtelbare Regelanweisung kann eine Eingrenzungsanweisung sein. Wenn eine Anfrage nicht mit der Scopedown-Aussage übereinstimmt, wird sie als nicht mit der Regelgruppen-Referenzaussage übereinstimmend AWS WAF bewertet, ohne sie anhand der Regelgruppe auszuwerten. Weitere Informationen zu Eingrenzungsanweisungen finden Sie unter [Eingrenzungsanweisungen](#).

Die Preise für die von Bot Control verwaltete Regelgruppe steigen mit der Anzahl der Webanfragen, die AWS WAF anhand der Regelgruppe ausgewertet werden. Sie können dazu beitragen, diese Kosten zu senken, indem Sie die Anzahl der Anfragen, die die Regelgruppe auswertet, mithilfe einer Scopedown-Erklärung einschränken. Möglicherweise möchten Sie beispielsweise zulassen, dass Ihre Homepage für alle geladen wird, auch für Bots, und dann die Regelgruppenregeln auf Anfragen anwenden, die an Ihre Anwendungs-APIs gehen oder einen bestimmten Inhaltstyp enthalten.

- **Labels und Regeln für den Label-Abgleich** — Sie können anpassen, wie die Bot-Control-Regelgruppe mit einem Teil des Bot-Traffics umgeht, den sie anhand der AWS WAF Label-Match-Rule-Anweisung identifiziert. Die Regelgruppe Bot Control fügt Ihren Webanfragen Labels hinzu. Sie können nach der Bot-Control-Regelgruppe Regeln für den Label-Abgleich hinzufügen, die den Bezeichnungen von Bot Control entsprechen, und die Behandlung anwenden, die Sie benötigen. Weitere Informationen zur Bezeichnung und zur Verwendung von Anweisungen zum Abgleich von Bezeichnungen finden Sie unter [Regelanweisung für Bezeichnungsübereinstimmung](#) und [AWS WAF Labels auf Webanfragen](#).
- **Benutzerdefinierte Anfragen und Antworten** — Sie können benutzerdefinierte Header zu Anfragen hinzufügen, die Sie zulassen, und Sie können benutzerdefinierte Antworten auf Anfragen senden, die Sie blockieren, indem Sie den Label-Abgleich mit den Funktionen für AWS WAF benutzerdefinierte Anfragen und Antworten kombinieren. Weitere Informationen zum Anpassen

von Anforderungen und Antworten finden Sie unter [Benutzerdefinierte Webanforderungen und Antworten in AWS WAF](#).

Warum Sie die Anwendungsintegrations-SDKs mit Bot Control verwenden sollten

Die meisten gezielten Schutzmaßnahmen der von Bot Control verwalteten Regelgruppe erfordern die Challenge-Token, die von den Anwendungsintegrations-SDKs generiert werden. Bei den Regeln, für die bei der Anfrage kein Challenge-Token erforderlich ist, handelt es sich um die Bot Control-Schutzmaßnahmen auf allgemeiner Ebene und um die Regeln für maschinelles Lernen auf zielgerichteter Ebene. Eine Beschreibung der Schutzstufen und Regeln in der Regelgruppe finden Sie unter [AWS WAF Regelgruppe „Bot-Kontrolle“](#).

Wir empfehlen dringend, die Anwendungsintegrations-SDKs zu implementieren, um die Bot-Control-Regelgruppe am effektivsten nutzen zu können. Das Challenge-Skript muss vor der Bot Control-Regelgruppe ausgeführt werden, damit die Regelgruppe von den Tokens, die das Skript erhält, profitieren kann.

- Mit den SDKs für die Anwendungsintegration wird das Skript automatisch ausgeführt.
- Wenn Sie die SDKs nicht verwenden können, können Sie Ihre Web-ACL so konfigurieren, dass sie die CAPTCHA Regelaktion Challenge oder für alle Anfragen ausführt, die von der Bot Control-Regelgruppe geprüft werden. Für die Verwendung der CAPTCHA Regelaktion Challenge oder können zusätzliche Gebühren anfallen. Details zu den Preisen finden Sie unter [AWS WAF -Preise](#).

Wenn Sie die Anwendungsintegrations-SDKs in Ihren Clients implementieren oder eine der Regelaktionen verwenden, mit denen das Challenge-Skript ausgeführt wird, erweitern Sie die Funktionen der Regelgruppe und die allgemeine Sicherheit Ihrer Client-Anwendung.

Tokens stellen bei jeder Webanfrage Client-Informationen bereit. Diese zusätzlichen Informationen ermöglichen es der Regelgruppe Bot Control, legitime Clientsitzungen von Clientsitzungen mit schlechtem Verhalten zu trennen, selbst wenn beide von einer einzigen IP-Adresse stammen. Die Regelgruppe verwendet die Informationen in den Tokens, um das Verhalten von Client-Sitzungsanfragen zu aggregieren und so die Erkennung und Abwehr zu optimieren, die die angestrebte Schutzstufe bietet.

Informationen zu den SDKs finden Sie unter [AWS WAF Integration von Client-Anwendungen](#)
Informationen zu AWS WAF Tokens finden Sie unter [AWS WAF Webanforderungstoken](#).
Informationen zu den Regelaktionen finden Sie unter [CAPTCHA und Challenge in AWS WAF](#).

Hinzufügen der von AWS WAF Bot Control verwalteten Regelgruppe zu Ihrer Web-ACL

Für die von Bot Control verwaltete Regelgruppe `AWSManagedRulesBotControlRuleSet` ist eine zusätzliche Konfiguration erforderlich, um die Schutzstufe zu identifizieren, die Sie implementieren möchten.

Eine Beschreibung der Regelgruppe und eine Liste der Regeln finden Sie unter [AWS WAF Regelgruppe „Bot-Kontrolle“](#).

Diese Anleitung richtet sich an Benutzer, die im Allgemeinen wissen, wie man Web-ACLs, Regeln und Regelgruppen für AWS WAF erstellt und verwaltet. Diese Themen werden in früheren Abschnitten dieses Handbuchs behandelt. Grundlegende Informationen zum Hinzufügen einer verwalteten Regelgruppe zu einer Web-ACL finden Sie unter [Hinzufügen einer verwalteten Regelgruppe zu einer Web-ACL über die Konsole](#).

Folgen Sie den bewährten Methoden

Verwenden Sie die Regelgruppe Bot Control gemäß den bewährten Methoden unter [Bewährte Methoden für intelligente Bedrohungsabwehr](#).

So verwenden Sie die Regelgruppe `AWSManagedRulesBotControlRuleSet` in einer Web-ACL

1. Fügen Sie die AWS verwaltete Regelgruppe `AWSManagedRulesBotControlRuleSet` zu Ihrer Web-ACL hinzu. Die vollständige Beschreibung der Regelgruppe finden Sie unter [the section called “Regelgruppe von Bot Control”](#).

Note

Ihnen werden zusätzliche Gebühren berechnet, wenn Sie diese verwaltete Regelgruppe verwenden. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).

Wenn Sie die Regelgruppe hinzufügen, bearbeiten Sie sie, um die Konfigurationsseite für die Regelgruppe zu öffnen.

2. Wählen Sie auf der Konfigurationsseite der Regelgruppe im Bereich Inspektionsebene die Inspektionsebene aus, die Sie verwenden möchten.
 - Häufig — Erkennt eine Vielzahl von sich selbst identifizierenden Bots, z. B. Web-Scraping-Frameworks, Suchmaschinen und automatisierte Browser. Bot-Control-Schutzmaßnahmen

auf dieser Ebene identifizieren häufig auftretende Bots mithilfe herkömmlicher Bot-Erkennungstechniken, wie z. B. der Analyse statischer Anforderungsdaten. Die Regeln kennzeichnen den Traffic dieser Bots und blockieren diejenigen, die sie nicht verifizieren können.

- **Gezielt** — Beinhaltet Schutzmaßnahmen auf allgemeiner Ebene und bietet eine gezielte Erkennung für ausgeklügelte Bots, die sich nicht selbst identifizieren. Gezielte Schutzmaßnahmen reduzieren Bot-Aktivitäten mithilfe einer Kombination aus Ratenbegrenzung und CAPTCHA sowie Browser-Herausforderungen im Hintergrund.
 - **TGT_**— Regeln, die gezielten Schutz bieten, haben Namen, die mit `TGT_` beginnen. Alle gezielten Schutzmaßnahmen verwenden Erkennungstechniken wie Browserabfragen, Fingerabdrücke und Verhaltensheuristiken, um bösartigen Bot-Traffic zu identifizieren.
 - **TGT_ML_**— Gezielte Schutzregeln, die maschinelles Lernen verwenden, haben Namen, die mit `TGT_ML_` beginnen. Diese Regeln verwenden automatisierte, maschinelle Lernanalysen der Besucherstatistiken von Websites, um ungewöhnliches Verhalten zu erkennen, das auf verteilte, koordinierte Bot-Aktivitäten hindeutet. AWS WAF analysiert Statistiken über Ihren Website-Verkehr wie Zeitstempel, Browsereigenschaften und die zuvor besuchte URL, um das maschinelle Lernmodell von Bot Control zu verbessern. Funktionen für maschinelles Lernen sind standardmäßig aktiviert, Sie können sie jedoch in Ihrer Regelgruppenkonfiguration deaktivieren. Wenn maschinelles Lernen deaktiviert ist, werden diese Regeln von AWS WAF nicht ausgewertet.
3. Wenn Sie die gezielte Schutzstufe verwenden und maschinelles Lernen (ML) nicht verwenden möchten, analysiert AWS WAF den Webverkehr auf verteilte, koordinierte Bot-Aktivitäten hin zu analysieren, deaktivieren Sie die Option für maschinelles Lernen. Maschinelles Lernen ist für die Bot-Kontrollregeln erforderlich, deren Namen mit `TGT_ML_` beginnen. Einzelheiten zu diesen Regeln finden Sie unter [Liste der Bot-Control-Regeln](#).
 4. Fügen Sie eine Erklärung zum Umfang der Regelgruppe hinzu, in der die Kosten für deren Verwendung aufgeführt sind. Eine Scope-down-Erklärung schränkt die Anzahl der Anfragen ein, die die Regelgruppe prüft. Beginnen Sie beispielsweise bei Anwendungsfällen mit und. [Beispiel für Bot Control: Verwenden Sie Bot Control nur für die Anmeldeseite](#) [Beispiel für Bot Control: Verwenden Sie Bot Control nur für dynamische Inhalte](#)
 5. Geben Sie alle zusätzlichen Konfigurationen an, die Sie für die Regelgruppe benötigen.
 6. Speichern Sie Ihre Änderungen an der Web-ACL.

Bevor Sie Ihre Bot-Control-Implementierung für den Produktionsdatenverkehr bereitstellen, sollten Sie sie in einer Staging- oder Testumgebung testen und optimieren, bis Sie mit den möglichen

Auswirkungen auf Ihren Datenverkehr vertraut sind. Testen und optimieren Sie dann die Regeln im Zählmodus mit Ihrem Produktionsdatenverkehr, bevor Sie sie aktivieren. Anleitungen finden Sie in den folgenden Abschnitten.

Falsche positive Ergebnisse mit AWS WAF Bot Control

Wir haben die Regeln in der von AWS WAF Bot Control verwalteten Regelgruppe sorgfältig ausgewählt, um Fehlalarme zu minimieren. Wir testen die Regeln anhand des globalen Datenverkehrs und überwachen ihre Auswirkungen auf Test-Web-ACLs. Es ist jedoch immer noch möglich, aufgrund von Änderungen der Verkehrsmuster Fehlalarme zu erhalten. Darüber hinaus ist bekannt, dass einige Anwendungsfälle zu Fehlalarmen führen und eine Anpassung an Ihren Web-Traffic erfordern.

Zu den Situationen, in denen Sie möglicherweise auf Fehlalarme stoßen, gehören die folgenden:

- Mobile Apps verfügen in der Regel über Benutzeragenten, die keine Browser sind. Diese werden von der `SignalNonBrowserUserAgent` Regel standardmäßig blockiert. Wenn Sie Traffic von mobilen Apps oder anderen legitimen Traffic mit Benutzeragenten erwarten, die keine Browser sind, müssen Sie eine Ausnahme hinzufügen, um dies zuzulassen.
- Möglicherweise sind Sie auf einen bestimmten Bot-Datenverkehr angewiesen, z. B. für die Überwachung der Betriebszeit, Integrationstests oder Marketing-Tools. Wenn Bot Control den Bot-Datenverkehr, den Sie zulassen möchten, identifiziert und blockiert, müssen Sie dies ändern, indem Sie eigene Regeln hinzufügen. Dies ist zwar nicht für alle Kunden ein falsch-positives Szenario, aber wenn es für Sie gilt, müssen Sie es genauso behandeln wie bei einem falsch positiven Szenario.
- Die von Bot Control verwaltete Regelgruppe verifiziert Bots anhand der IP-Adressen von AWS WAF. Wenn Sie Bot Control verwenden und verifizierte Bots haben, die durch einen Proxy oder Load Balancer geleitet werden, müssen Sie sie ggf. explizit mit einer benutzerdefinierten Regel zulassen. Informationen zum Erstellen einer benutzerdefinierten Regel dieses Typs finden Sie unter [Weitergeleitete IP-Adresse](#).
- Eine Bot-Control-Regel mit einer niedrigen globalen Falsch-Positiv-Rate kann sich stark auf bestimmte Geräte oder Anwendungen auswirken. Bei den Tests und der Validierung wurden beispielsweise Anforderungen von Anwendungen mit geringem Datenverkehrsaufkommen oder von weniger verbreiteten Browsern oder Geräten möglicherweise nicht berücksichtigt.
- Eine Bot-Control-Regel mit einer historisch niedrigen Falsch-Positiv-Rate könnte die Zahl der Falschmeldungen bei gültigem Traffic erhöht haben. Dies könnte auf neue Datenverkehrsmuster oder Anforderungsattribute zurückzuführen sein, die mit gültigem Datenverkehr auftauchen und

dazu führen, dass eine Übereinstimmung mit der Regel vorliegt, wo dies vorher nicht der Fall war. Solche Veränderungen können auf Situationen wie folgende zurückzuführen sein:

- Details des Datenverkehrs, die sich ändern, wenn der Datenverkehr durch Netzwerkanwendungen wie Load Balancer oder Content Distribution Networks (CDN) fließt
- Neue Veränderungen an den Datenverkehrsdaten, z. B. neue Browser oder neue Versionen von bestehenden Browsern

Informationen zum Umgang mit Fehlalarmen, die Sie möglicherweise von der verwalteten Regelgruppe „AWS WAF Bot Control“ erhalten, finden Sie in den Anleitungen im folgenden Abschnitt [Testen und Bereitstellen von AWS WAF Bot Control](#).

Testen und Bereitstellen von AWS WAF Bot Control

Dieser Abschnitt enthält allgemeine Anleitungen zum Konfigurieren und Testen einer AWS WAF Bot Control-Implementierung für Ihre Site. Die spezifischen Schritte, die Sie befolgen, hängen von Ihren Bedürfnissen, Ressourcen und den Webanfragen ab, die Sie erhalten.

Diese Informationen sind zusätzlich zu den allgemeinen Informationen zum Testen und Optimieren verfügbar, die Sie unter finden [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

Note

AWS Verwaltete Regeln wurden entwickelt, um Sie vor gängigen Internet-Bedrohungen zu schützen. Wenn sie gemäß der Dokumentation verwendet werden, bieten Regelgruppen mit AWS verwalteten Regeln eine weitere Sicherheitsebene für Ihre Anwendungen. Regelgruppen mit AWS verwalteten Regeln sind jedoch nicht als Ersatz für Ihre Sicherheitsaufgaben gedacht, die durch die von Ihnen ausgewählten AWS Ressourcen bestimmt werden. Anhand des [Modells der gemeinsamen Verantwortung](#) können Sie sicherstellen, dass Ihre Ressourcen ordnungsgemäß geschützt AWS sind.

Risiken rund um Produktionsdatenverkehr

Bevor Sie Ihre Bot-Control-Implementierung für den Produktionsdatenverkehr bereitstellen, sollten Sie sie in einer Staging- oder Testumgebung testen und optimieren, bis Sie mit den möglichen Auswirkungen auf Ihren Datenverkehr vertraut sind. Testen und optimieren Sie dann die Regeln im Zählmodus mit Ihrem Produktionsdatenverkehr, bevor Sie sie aktivieren.

Diese Anleitung richtet sich an Benutzer, die im Allgemeinen wissen, wie man Web-ACLs, Regeln und Regelgruppen für AWS WAF erstellt und verwaltet. Diese Themen werden in früheren Abschnitten dieses Handbuchs behandelt.

So konfigurieren und testen Sie eine Bot-Control-Implementierung

Führen Sie diese Schritte zuerst in einer Testumgebung und dann in der Produktion aus.

1. Hinzugen der verwalteten Bot-Control-Regelgruppe

Note

Wenn Sie diese verwaltete Regelgruppe verwenden, werden Ihnen zusätzliche Gebühren berechnet. Weitere Informationen finden Sie unter [AWS WAF - Preisgestaltung](#).

Fügen Sie die verwaltete AWS Regelgruppe `AWSManagedRulesBotControlRuleSet` einer neuen oder vorhandenen Web-ACL hinzu und konfigurieren Sie sie so, dass sie das aktuelle Verhalten der Web-ACL nicht verändert.

- Wenn Sie die verwaltete Regelgruppe hinzufügen, bearbeiten Sie sie und gehen Sie wie folgt vor:
 - Wählen Sie im Bereich Inspektionsebene die Inspektionsebene aus, die Sie verwenden möchten.
 - Häufig — Erkennt eine Vielzahl von sich selbst identifizierenden Bots, z. B. Web-Scraping-Frameworks, Suchmaschinen und automatisierte Browser. Bot-Control-Schutzmaßnahmen auf dieser Ebene identifizieren häufig auftretende Bots mithilfe herkömmlicher Bot-Erkennungstechniken, wie z. B. der Analyse statischer Anforderungsdaten. Die Regeln kennzeichnen den Traffic dieser Bots und blockieren diejenigen, die sie nicht verifizieren können.
 - Gezielt — Beinhaltet Schutzmaßnahmen auf allgemeiner Ebene und bietet eine gezielte Erkennung für ausgeklügelte Bots, die sich nicht selbst identifizieren. Gezielte Schutzmaßnahmen reduzieren Bot-Aktivitäten mithilfe einer Kombination aus Ratenbegrenzung und CAPTCHA sowie Browser-Herausforderungen im Hintergrund.

- **TGT_**— Regeln, die gezielten Schutz bieten, haben Namen, die mit **TGT_** beginnen. Alle gezielten Schutzmaßnahmen verwenden Erkennungstechniken wie Browserabfragen, Fingerabdrücke und Verhaltensheuristiken, um böartigen Bot-Traffic zu identifizieren.
- **TGT_ML_**— Gezielte Schutzregeln, die maschinelles Lernen verwenden, haben Namen, die mit **TGT_ML_** beginnen. Diese Regeln verwenden automatisierte, maschinelle Lernanalysen der Besucherstatistiken von Websites, um ungewöhnliches Verhalten zu erkennen, das auf verteilte, koordinierte Bot-Aktivitäten hindeutet. AWS WAF analysiert Statistiken über Ihren Website-Verkehr wie Zeitstempel, Browsereigenschaften und die zuvor besuchte URL, um das maschinelle Lernmodell von Bot Control zu verbessern. Funktionen für maschinelles Lernen sind standardmäßig aktiviert, Sie können sie jedoch in Ihrer Regelgruppenkonfiguration deaktivieren. Wenn maschinelles Lernen deaktiviert ist, werden diese Regeln von AWS WAF nicht ausgewertet.

Weitere Informationen zu dieser Option finden Sie unter [AWS WAF Regelgruppe „Bot-Kontrolle“](#).

- Öffnen Sie im Bereich Regeln die Dropdownliste Alle Regelaktionen außer Kraft setzen und wählen Sie aus Count. Bei dieser Konfiguration werden Anfragen anhand aller Regeln in der Regelgruppe von AWS WAF ausgewertet und nur die Treffer gezählt, die sich daraus ergeben, wobei Anfragen trotzdem Labels hinzugefügt werden. Weitere Informationen finden Sie unter [Regelaktionen in einer Regelgruppe überschreiben](#).

Mit dieser Überschreibung können Sie die potenziellen Auswirkungen der Bot-Kontrollregeln auf Ihren Traffic überwachen und so bestimmen, ob Sie Ausnahmen für Dinge wie interne Anwendungsfälle oder gewünschte Bots hinzufügen möchten.

- Positionieren Sie die Regelgruppe so, dass sie in der Web-ACL als Letztes ausgewertet wird, mit einer Prioritätseinstellung, die numerisch höher ist als alle anderen Regeln oder Regelgruppen, die Sie bereits verwenden. Weitere Informationen finden Sie unter [Reihenfolge der Verarbeitung von Regeln und Regelgruppen in einer Web-ACL](#).

Auf diese Weise wird Ihre derzeitige Handhabung des Datenverkehrs nicht gestört. Wenn Sie beispielsweise Regeln haben, die böartigen Datenverkehr wie SQL-Injection oder Cross-Site-Scripting erkennen, werden diese Anfragen weiterhin erkannt und protokolliert. Wenn Sie über Regeln verfügen, die bekannten nicht böswilligen Datenverkehr zulassen, lassen diese derartigen Datenverkehr weiterhin zu, ohne dass er von der durch Bot Control verwalteten Regelgruppe blockiert wird. Möglicherweise möchten Sie die Verarbeitungsreihenfolge während Ihrer Test- und Optimierungsaktivitäten anpassen, aber das ist ein guter Anfang.

2. Aktivieren von Sampling, Protokollierung und Metriken für die Web-ACL

Konfigurieren Sie bei Bedarf die Protokollierung für die Web-ACL und aktivieren Sie Sampling und CloudWatch Amazon-Metriken. Sie können Metriken und Protokollierung verwenden, um die Interaktion Ihres Webverkehrs mit der von Bot Control verwalteten Regelgruppe zu überwachen.

- Weitere Informationen zum Konfigurieren und Verwenden der Protokollierung finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).
- Informationen zu CloudWatch Amazon-Metriken finden Sie unter [Überwachung mit Amazon CloudWatch](#).
- Informationen zum Sampling von Webanforderungen finden Sie unter [Anzeigen einer Stichprobe von Webanforderungen](#).

3. Zuordnen der Web-ACL zu einer Ressource

Wenn die Web-ACL noch keiner Ressource zugeordnet ist, ordnen Sie sie zu. Weitere Informationen finden Sie unter [Zuordnen oder Aufheben der Zuordnung einer Web-ACL zu einer Ressource AWS](#).

4. Überwachung von Datenverkehr und Bot-Control-Regelübereinstimmungen

Stellen Sie sicher, dass Datenverkehr fließt und dass durch die Regeln der durch Bot Control verwalteten Regelgruppe Bezeichnungen zu übereinstimmenden Webanforderungen hinzugefügt werden. Sie können die Labels in den Protokollen und die Bot- und Label-Metriken in den CloudWatch Amazon-Metriken sehen. In den Protokollen werden die Regeln, die Sie zur Zählung in der Regelgruppe außer Kraft gesetzt haben, in der Liste mit auf zählen action gesetzt und ruleGroupList mit der overriddenAction Angabe der konfigurierten Regelaktion angezeigt, die Sie überschrieben haben.

Note

Die verwaltete Bot-Control-Regelgruppe überprüft Bots, die die IP-Adressen von AWS WAF verwenden. Wenn Sie Bot Control verwenden und verifizierte Bots haben, die durch einen Proxy oder Load Balancer geleitet werden, müssen Sie sie ggf. explizit mit einer benutzerdefinierten Regel zulassen. Informationen zum Erstellen einer benutzerdefinierten Regel finden Sie unter [Weitergeleitete IP-Adresse](#). Informationen darüber, wie Sie die Regel verwenden können, um die Behandlung von Webanforderungen durch Bot Control anzupassen, finden Sie im nächsten Schritt.

Überprüfen Sie die Verarbeitung von Webanfragen sorgfältig auf Fehlalarme, die Sie möglicherweise durch eine benutzerdefinierte Behandlung abmildern müssen. Beispiele für falsch positive Ergebnisse finden Sie unter [Falsche positive Ergebnisse mit AWS WAF Bot Control](#).

5. Anpassen der Behandlung von Webanforderungen durch Bot Control

Fügen Sie bei Bedarf Ihre eigenen Regeln hinzu, die Anforderungen explizit zulassen oder blockieren. Dadurch ändern Sie, wie Bot-Control-Regeln andernfalls damit umgehen würden.

Wie Sie dies tun, hängt von Ihrem Anwendungsfall ab, aber die folgenden Lösungen sind üblich:

- Erlauben Sie Anforderungen explizit mit einer Regel, die Sie vor der verwalteten Bot-Control-Regelgruppe hinzufügen. Auf diese Weise gelangen die zugelassenen Anforderungen niemals zur Auswertung durch die Regelgruppe. Dies kann dazu beitragen, die Kosten für die Verwendung der verwalteten Bot-Control-Regelgruppe einzudämmen.
- Schließen Sie Anfragen von der Bewertung durch Bot Control aus, indem Sie der Anweisung für verwaltete Regelgruppen von Bot Control eine Scopedown-Aussage hinzufügen. Das funktioniert genauso wie die vorherige Option. Dadurch können Sie die Kosten für die Verwendung der verwalteten Bot-Control-Regelgruppe eindämmen, da die Anforderungen, die nicht der Eingrenzungsanweisung entsprechen, nie zur Auswertung durch die Regelgruppe gelangen. Informationen zu Eingrenzungsanweisungen finden Sie unter [Eingrenzungsanweisungen](#).

-Beispiele finden Sie nachfolgend.

- [IP-Bereich von der Bot-Verwaltung ausschließen](#)
- [Traffic von einem Bot zulassen, den Sie steuern](#)
- Verwenden Sie Bot Control-Bezeichnungen bei der Behandlung von Anforderungen, um Anforderungen zuzulassen oder zu blockieren. Fügen Sie nach der verwalteten Bot-Control-Regelgruppe eine Regel für einen Bezeichnungsabgleich hinzu, um Anforderungen mit Bezeichnungen, die Sie zulassen möchten, von denen zu trennen, die Sie blockieren möchten.

Behalten Sie nach dem Testen die zugehörigen Bot-Control-Regeln im Zählmodus und die Entscheidungen zur Anforderungsbehandlung in Ihrer benutzerdefinierten Regel.

Informationen zu Anweisungen für Bezeichnungsabgleiche finden Sie unter [Regelanweisung für Bezeichnungsübereinstimmung](#).

Beispiele für diese Art der Anpassung finden Sie im Folgenden:

- [Ausnahme für einen blockierten User Agent erstellen](#)
- [Bestimmten blockierten Bot zulassen](#)
- [Verifizierte Bots blockieren](#)

Weitere Beispiele finden Sie unter [AWS WAF Beispiele für Bot-Kontrolle](#).

6. Aktivieren Sie bei Bedarf die Einstellungen der verwalteten Bot-Control-Regelgruppe

Abhängig von Ihrer Situation haben Sie sich möglicherweise dafür entschieden, einige Bot-Kontrollregeln im Zählmodus oder mit einer anderen Aktionsüberschreibung zu belassen. Aktivieren Sie für die Regeln, die Sie so ausführen lassen möchten, wie sie innerhalb der Regelgruppe konfiguriert sind, die reguläre Regelkonfiguration. Bearbeiten Sie dazu die Regelgruppenanweisung in Ihrer Web-ACL und nehmen Sie Ihre Änderungen im Bereich Regeln vor.

AWS WAF Beispiele für Bot-Kontrolle

Dieser Abschnitt zeigt Beispielkonfigurationen, die eine Vielzahl gängiger Anwendungsfälle für AWS WAF Bot Control-Implementierungen erfüllen.

Jedes Beispiel enthält eine Beschreibung des Anwendungsfalls und zeigt dann in JSON-Auflistungen die Lösung für die benutzerdefiniert konfigurierten Regeln an.

Note

Die in diesen Beispielen gezeigten JSON-Auflistungen wurden in der Konsole erstellt, indem die Regel konfiguriert und dann mit dem Rule JSON editor (JSON-Regel-Editor) bearbeitet wurde.

Themen

- [Beispiel Bot Control: Einfache Konfiguration](#)
- [Beispiel für Bot-Kontrolle: Verifizierte Bots explizit zulassen](#)
- [Beispiel für Bot-Kontrolle: Verifizierte Bots blockieren](#)
- [Beispiel für Bot-Kontrolle: Einen bestimmten blockierten Bot zulassen](#)

- [Beispiel für Bot-Kontrolle: Erstellen Sie eine Ausnahme für einen blockierten Benutzeragenten](#)
- [Beispiel für Bot Control: Verwenden Sie Bot Control nur für die Anmeldeseite](#)
- [Beispiel für Bot Control: Verwenden Sie Bot Control nur für dynamische Inhalte](#)
- [Beispiel für Bot-Kontrolle: IP-Bereich von der Bot-Verwaltung ausschließen](#)
- [Beispiel für Bot-Kontrolle: Erlaube Traffic von einem Bot, den du kontrollierst](#)
- [Beispiel für Bot-Kontrolle: Gezielte Inspektionsstufe](#)
- [Beispiel für Bot-Kontrolle: Verwenden Sie zwei Anweisungen, um die Verwendung der angestrebten Inspektionsebene einzuschränken](#)

Beispiel Bot Control: Einfache Konfiguration

Die folgende JSON-Liste zeigt ein Beispiel für eine Web-ACL mit einer von AWS WAF Bot Control verwalteten Regelgruppe. Beachten Sie die Sichtbarkeitskonfiguration, die AWS WAF dazu führt, dass Anforderungsmuster und Metriken zu Überwachungszwecken gespeichert werden.

```
{
  "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
}

```

Beispiel für Bot-Kontrolle: Verifizierte Bots explizit zulassen

AWS WAF Bot Control blockiert keine Bots, von denen bekannt ist, dass AWS sie häufig vorkommen und verifizierbar sind. Wenn Bot Control eine Webanforderung als von einem verifizierten Bot stammend identifiziert, fügt es eine Bezeichnung hinzu, die den Bot benennt, sowie eine Bezeichnung, die angibt, dass es sich um einen verifizierten Bot handelt. Bot Control fügt keine anderen Bezeichnungen hinzu, wie z. B. Signalbezeichnungen, um zu verhindern, dass bekannte gute Bots blockiert werden.

Möglicherweise haben Sie andere AWS WAF Regeln, die verifizierte Bots blockieren. Wenn Sie sicherstellen möchten, dass verifizierte Bots zugelassen werden, fügen Sie eine benutzerdefinierte Regel hinzu, um sie auf der Grundlage der Bezeichnungen von Bot Control zuzulassen. Die neue Regel muss nach der verwalteten Bot-Control-Regelgruppe ausgeführt werden, damit die Bezeichnungen für den Abgleich verfügbar sind.

Die folgende Regel erlaubt explizit verifizierte Bots.

```

{
  "Name": "match_rule",
  "Statement": {
    "LabelMatchStatement": {
      "Scope": "LABEL",

```

```

    "Key": "awswaf:managed:aws:bot-control:bot:verified"
  }
},
"RuleLabels": [],
"Action": {
  "Allow": {}
}
}

```

Beispiel für Bot-Kontrolle: Verifizierte Bots blockieren

Zum Blockieren verifizierter Bots müssen Sie eine Regel hinzufügen, die nach der verwalteten AWS WAF -Bot-Control-Regelgruppe ausgeführt wird, um sie zu blockieren. Identifizieren Sie dazu die Namen der Bots, die Sie blockieren möchten, und verwenden Sie eine Anweisung für den Bezeichnungsabgleich, um sie zu identifizieren und zu blockieren. Wenn Sie nur alle verifizierten Bots blockieren möchten, können Sie den Abgleich mit der `bot:name:-` Bezeichnung weglassen.

Die folgende Regel blockiert nur den verifizierten Bot `bingbot`. Diese Regel muss nach der verwalteten Bot-Control-Regelgruppe ausgeführt werden.

```

{
  "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": {}
  }
}

```

```
}  
}
```

Die folgende Regel blockiert alle verifizierten Bots.

```
{  
  "Name": "match_rule",  
  "Statement": {  
    "LabelMatchStatement": {  
      "Scope": "LABEL",  
      "Key": "aws:waf:managed:aws:bot-control:bot:verified"  
    }  
  },  
  "RuleLabels": [],  
  "Action": {  
    "Block": {}  
  }  
}
```

Beispiel für Bot-Kontrolle: Einen bestimmten blockierten Bot zulassen

Es ist möglich, dass ein Bot durch mehr als eine der Bot-Control-Regeln blockiert wird. Führen Sie für jede Blockierungsregel die folgenden Schritte aus.

Wenn eine AWS WAF Bot-Kontrollregel einen Bot blockiert, den Sie nicht blockieren möchten, gehen Sie wie folgt vor:

1. Identifizieren Sie die Bot-Control-Regel, die den Bot blockiert, in den Protokollen. Die Blockierungsregel wird in den Protokollen in den Feldern angegeben, deren Namen mit `terminatingRule` beginnen. Informationen zu den Web-ACL-Protokollen finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#). Merken Sie sich die Bezeichnung, die die Regel den Anforderungen hinzufügt.
2. Überschreiben Sie in Ihrer Web-ACL die Aktion der Blockierungsregel, sodass sie zählt. Bearbeiten Sie dazu in der Konsole die Regelgruppenregel in der Web-ACL und wählen Sie Count für die Regel eine Regelaktion außer Kraft setzen. Dadurch wird sichergestellt, dass der Bot nicht durch die Regel blockiert wird, aber die Regel wendet ihre Bezeichnung trotzdem auf übereinstimmende Anfragen an.
3. Fügen Sie Ihrer Web-ACL nach der verwalteten Bot-Control-Regelgruppe eine Regel für den Bezeichnungsabgleich hinzu. Konfigurieren Sie die Regel so, dass sie mit der Bezeichnung

der überschriebenen Regel übereinstimmt und alle passenden Anfragen blockiert werden, mit Ausnahme des Bots, den Sie nicht blockieren möchten.

Die Web-ACL ist nun so konfiguriert, dass der Bot, den Sie zulassen möchten, nicht mehr von der Blockierungsregel blockiert wird, die Sie anhand der Protokolle identifiziert haben.

Überprüfen Sie den Datenverkehr und die Protokolle erneut, um sicherzugehen, dass der Bot durchgelassen wird. Sollte das nicht der Fall sein, führen Sie die oben genannten Schritte erneut durch.

Angenommen, Sie möchten alle Überwachungs-Bots mit Ausnahme von pingdom blockieren. In diesem Fall überschreiben Sie die `CategoryMonitoring` Regel, um zu zählen, und schreiben dann eine Regel, um alle überwachenden Bots außer denen mit dem Bot-Namen zu blockieren. `pingdom`

Die folgende Regel verwendet die von Bot Control verwaltete Regelgruppe, setzt jedoch die Regelaktion für `CategoryMonitoring` das Zählen außer Kraft. Die Kategorieüberwachungsregel wendet ihre Bezeichnungen wie üblich auf übereinstimmende Anforderungen an, zählt sie aber nur, anstatt die übliche Blockierungsaktion auszuführen.

```
{
  "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"
}
}

```

Die folgende Regel führt einen Abgleich mit der Bezeichnung für die Kategorieüberwachung durch, die die vorangehende Regel `CategoryMonitoring` zu passenden Webanforderungen hinzufügt. Unter den Anforderungen der Kategorieüberwachung blockiert diese Regel alle bis auf diejenigen, die eine Bezeichnung für den Botnamen `pingdom` haben.

Die folgende Regel muss in der Verarbeitungsreihenfolge der Web-ACLs nach der vorhergehenden verwalteten Bot-Control-Regelgruppe ausgeführt werden.

```

{
  "Name": "match_rule",
  "Priority": 10,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awsmaf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awsmaf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        }
      ]
    }
  }
},

```

```

    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "match_rule"
    }
  }
}

```

Beispiel für Bot-Kontrolle: Erstellen Sie eine Ausnahme für einen blockierten Benutzeragenten

Wenn der Datenverkehr von Benutzeragenten, die keine Browser sind, fälschlicherweise blockiert wird, können Sie eine Ausnahme erstellen, indem Sie die betreffende AWS WAF Bot-Kontrollregel `SignalNonBrowserUserAgent` auf `Count` setzen und dann die Bezeichnung der Regel mit Ihren Ausnahmekriterien kombinieren.

Note

Mobile Apps verfügen in der Regel über Benutzeragenten, die keine Browser sind. Diese werden von der `SignalNonBrowserUserAgent` Regel standardmäßig blockiert.

Die folgende Regel verwendet die von Bot Control verwaltete Regelgruppe, überschreibt jedoch die Regelaktion für `SignalNonBrowserUserAgent` To Count. Die Signalregel wendet ihre Bezeichnungen wie üblich auf übereinstimmende Anforderungen an, zählt sie aber nur, anstatt die übliche Blockierungsaktion auszuführen.

```

{
  "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"
}
}

```

Die folgende Regel entspricht der Signalbezeichnung, die die `SignalNonBrowserUserAgent` Bot-Control-Regel ihren entsprechenden Webanfragen hinzufügt. Unter den Signalanfragen blockiert diese Regel alle bis auf diejenigen, die den Benutzeragenten haben, den wir zulassen möchten.

Die folgende Regel muss in der Verarbeitungsreihenfolge der Web-ACLs nach der vorhergehenden verwalteten Bot-Control-Regelgruppe ausgeführt werden.

```

{
  "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"
}
}
```

Beispiel für Bot Control: Verwenden Sie Bot Control nur für die Anmeldeseite

Das folgende Beispiel verwendet eine Scopedown-Anweisung, um AWS WAF Bot Control nur auf Traffic anzuwenden, der auf die Anmeldeseite einer Website gelangt, die durch den URI-Pfad identifiziert wird. `login` Der URI-Pfad zu Ihrer Anmeldeseite kann sich je nach Anwendung und Umgebung von diesem Beispiel unterscheiden.

```
{
  "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"
}
}
}
```

Beispiel für Bot Control: Verwenden Sie Bot Control nur für dynamische Inhalte

In diesem Beispiel wird eine Scopedown-Anweisung verwendet, um AWS WAF Bot Control nur auf dynamische Inhalte anzuwenden.

Die Eingrenzungsanweisung schließt statische Inhalte aus, indem sie die Abgleichsergebnisse für einen Regex-Mustersatz negiert:

- Der Regex-Mustersatz ist so konfiguriert, dass er auf Erweiterungen von statischen Inhalten passt. Die Spezifikation des Regex-Mustersatzes könnte zum Beispiel `(?i)\.(jpe?g|gif|png|svg|`

ico|css|js|woff2?)\$ sein. Informationen zu Regex-Mustersätzen und -anweisungen finden Sie unter [Regex-Mustersatz Übereinstimmungsregeln](#).

- In der Eingrenzungsanweisung wird der übereinstimmende statische Inhalt ausgeschlossen, indem die Regex-Mustersatzanweisung in eine NOT-Anweisung geschachtelt wird. Informationen zu dieser NOT-Anweisung finden Sie unter [NOT-Regelanweisung](#).

```
{
  "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"
          }
        ]
      }
    }
  }
}
```

```
    }  
  ]  
}  
}  
}  
}  
}
```

Beispiel für Bot-Kontrolle: IP-Bereich von der Bot-Verwaltung ausschließen

Wenn Sie eine Teilmenge des Web-Traffics aus der Verwaltung von AWS WAF Bot Control ausschließen möchten und Sie diese Teilmenge anhand einer Regelanweisung identifizieren können, schließen Sie sie aus, indem Sie Ihrer von Bot Control verwalteten Regelgruppe eine Scopedown-Anweisung hinzufügen.

Die folgende Regel führt die normale Bot-Control-Verwaltung für den gesamten Webdatenverkehr durch, mit Ausnahme von Webanforderungen, die von einem bestimmten IP-Adressbereich stammen.

```
{  
  "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"
      }
    }
  }
}
}
}
}
}

```

Beispiel für Bot-Kontrolle: Erlaube Traffic von einem Bot, den du kontrollierst

Sie können einige Website-Überwachungsbots und benutzerdefinierte Bots so konfigurieren, dass sie benutzerdefinierte Header senden. Wenn Sie Traffic von diesen Arten von Bots zulassen möchten, können Sie sie so konfigurieren, dass sie einem Header ein gemeinsames Geheimnis hinzufügen. Anschließend können Sie Nachrichten mit dem Header ausschließen, indem Sie der Anweisung für verwaltete Regelgruppen von AWS WAF Bot Control eine Scopedown-Anweisung hinzufügen.

Die folgende Beispielregel schließt Datenverkehr mit einem geheimen Header von der Prüfung durch Bot Control aus.

```

{
  "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"
          }
        }
      }
    }
  }
}
}
}
}
}
}

```

Beispiel für Bot-Kontrolle: Gezielte Inspektionsstufe

Für ein verbessertes Schutzniveau können Sie die gezielte Inspektionsstufe in Ihrer von AWS WAF Bot Control verwalteten Regelgruppe aktivieren.

Im folgenden Beispiel sind Funktionen für maschinelles Lernen aktiviert. Sie können dieses Verhalten deaktivieren, indem Sie `EnableMachineLearning` auf `false` einstellen.

```

{
  "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"
}
}
}
```

Beispiel für Bot-Kontrolle: Verwenden Sie zwei Anweisungen, um die Verwendung der angestrebten Inspektionsebene einzuschränken

Zur Kostenoptimierung können Sie in Ihrer Web-ACL zwei von AWS WAF Bot Control verwaltete Regelgruppenanweisungen mit unterschiedlichen Prüfungsebenen und Geltungsbereichen verwenden. Sie könnten beispielsweise die Anweisung zur Zielinspektionsebene nur auf sensiblere Anwendungsendpunkte beschränken.

Die beiden Aussagen im folgenden Beispiel schließen sich gegenseitig aus. Ohne diese Konfiguration könnte eine Anfrage zu zwei kostenpflichtigen Evaluierungen führen.

Note

Die Referenzierung `AWSManagedRulesBotControlRuleSet` mehrerer Anweisungen wird im Visual Editor in der Konsole nicht unterstützt. Verwenden Sie stattdessen den JSON-Editor.

```
{
  "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 Integration von Client-Anwendungen

Verwenden Sie APIs zur Integration von AWS WAF Client-Anwendungen, um den clientseitigen Schutz mit Ihrem AWS serverseitigen Web-ACL-Schutz zu verknüpfen. So können Sie überprüfen, ob es sich bei den Client-Anwendungen, die Webanfragen an Ihre geschützten Ressourcen senden, um die vorgesehenen Clients handelt und dass es sich bei Ihren Endbenutzern um Menschen handelt.


Verwenden Sie die Client-Integrationen, um Browser-Herausforderungen und CAPTCHA-Rätsel im Hintergrund zu bewältigen, Tokens mit dem Nachweis erfolgreicher Browser- und Endbenutzerantworten zu erhalten und diese Token in Anfragen an Ihre geschützten Endgeräte aufzunehmen. Allgemeine Informationen AWS WAF zu Tokens finden Sie unter [AWS WAF Webanforderungstoken](#)

Kombinieren Sie Ihre Client-Integrationen mit Web-ACL-Schutzmaßnahmen, für die gültige Token für den Zugriff auf Ihre Ressourcen erforderlich sind. Sie können Regelgruppen verwenden, die Challenge-Token prüfen und überwachen, wie sie im nächsten Abschnitt unter aufgeführt sind [Intelligente Bedrohungsintegration und AWS verwaltete Regeln](#), und Sie können die Aktionen CAPTCHA und Challenge Regeln zur Überprüfung verwenden, wie unter beschrieben. [CAPTCHA und Challenge in AWS WAF](#)

AWS WAF bietet zwei Integrationsebenen für JavaScript Anwendungen und eine für mobile Anwendungen:

- Intelligente Integration von Bedrohungen — Überprüfen Sie die Client-Anwendung und sorgen Sie für die Erfassung und Verwaltung von AWS Tokens. Dies ähnelt der Funktionalität, die durch die AWS WAF Challenge Regelaktion bereitgestellt wird. Diese Funktionalität integriert Ihre Client-Anwendung vollständig in die `AWSManagedRulesACFPRuleSet` verwaltete Regelgruppe, die `AWSManagedRulesATPRuleSet` verwaltete Regelgruppe und die Zielschutzebene der `AWSManagedRulesBotControlRuleSet` verwalteten Regelgruppe.


Die intelligenten Threat-Integrations-APIs stellen mithilfe der AWS WAF Silent Browser Challenge sicher, dass Anmeldeversuche und andere Aufrufe Ihrer geschützten Ressource erst zulässig sind, nachdem der Client ein gültiges Token erworben hat. Die APIs verwalten die Token-Autorisierung für Ihre Client-Anwendungssitzungen und sammeln Informationen über den Client, um festzustellen, ob er von einem Bot oder von einem Menschen betrieben wird.

 Note

Dies ist für JavaScript und für mobile Android- und iOS-Anwendungen verfügbar.

- CAPTCHA-Integration — Verifizieren Sie Endbenutzer mit einem maßgeschneiderten CAPTCHA-Puzzle, das Sie in Ihrer Anwendung verwalten. Dies ähnelt der Funktionalität, die durch die AWS WAF CAPTCHA Regelaktion bereitgestellt wird, bietet jedoch zusätzliche Kontrolle über die Platzierung und das Verhalten der Rätsel.

Diese Integration nutzt die JavaScript intelligente Bedrohungsintegration, um Herausforderungen im Hintergrund auszuführen und AWS WAF Tokens auf der Kundenseite bereitzustellen.

 Note

Dies ist für JavaScript Anwendungen verfügbar.

Themen

- [Intelligente Bedrohungsintegration und AWS verwaltete Regeln](#)
- [Zugriff auf die Integrations-APIs](#)
- [AWS WAF JavaScript Integrationen](#)
- [AWS WAF Integration mobiler Anwendungen](#)

Intelligente Bedrohungsintegration und AWS verwaltete Regeln

Die Intelligent Threat Integration APIs arbeiten mit Web-ACLs zusammen, die die intelligenten Bedrohungsregelgruppen verwenden, um die volle Funktionalität dieser erweiterten verwalteten Regelgruppen zu ermöglichen.

- AWS WAF Verwaltete Regelgruppe zur Erstellung von Fraud Control-Konten zur Betrugsprävention (ACFP). `AWSManagedRulesACFPRuleSet`

Betrug bei der Kontoerstellung ist eine illegale Online-Aktivität, bei der ein Angreifer ungültige Konten in Ihrer Anwendung erstellt, um beispielsweise Anmeldeboni zu erhalten oder sich als jemand auszugeben. Die verwaltete ACFP-Regelgruppe bietet Regeln zum Blockieren, Kennzeichnen und Verwalten von Anfragen, die Teil betrügerischer Kontoerstellungsversuche sein könnten. Die APIs ermöglichen eine fein abgestimmte Überprüfung des Client-Browsers und Informationen zur Benutzerinteraktivität, anhand derer die ACFP-Regeln gültigen Client-Verkehr von böartigem Datenverkehr trennen.

Weitere Informationen finden Sie unter [AWS WAF Regelgruppe Betrugsprävention \(ACFP\) zur Kontoerstellung bei der Betrugsbekämpfung](#) und [AWS WAF Einrichtung von Konten bei der Betrugsbekämpfung und Betrugsprävention \(ACFP\)](#).

- AWS WAF Verwaltete Regelgruppe zur Verhinderung von Kontoübernahmen (ATP) bei der Betrugsbekämpfung. `AWSManagedRulesATPRuleSet`

Kontoübernahmen sind eine illegale Online-Aktivität, bei der sich ein Angreifer unbefugten Zugriff auf das Konto einer anderen Person verschafft. Die von ATP verwaltete Regelgruppe bietet Regeln zum Blockieren, Kennzeichnen und Verwalten von Anfragen, die Teil böswilliger Kontoübernahmeversuche sein könnten. Die APIs ermöglichen eine fein abgestimmte Client-Überprüfung und Verhaltensaggregation, anhand derer die ATP-Regeln gültigen Client-Verkehr von böartigem Datenverkehr trennen.

Weitere Informationen finden Sie unter [AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen \(ATP\) zur Betrugsbekämpfung](#) und [AWS WAF Verhinderung von Kontoübernahmen bei der Betrugsbekämpfung \(ATP\)](#).

- Gezielte Schutzstufe der von AWS WAF Bot Control verwalteten Regelgruppe. `AWSManagedRulesBotControlRuleSet`

Die Palette der Bots reicht von selbstidentifizierenden und nützlichen Bots, wie die meisten Suchmaschinen und Crawler, bis hin zu böartigen Bots, die Ihre Website angreifen und sich nicht selbst identifizieren. Die verwaltete Regelgruppe von Bot Control bietet Regeln zur Überwachung, Kennzeichnung und Verwaltung der Bot-Aktivitäten in Ihrem Web-Traffic. Wenn Sie die gezielte Schutzstufe dieser Regelgruppe verwenden, verwenden die gezielten Regeln die von den APIs bereitgestellten Client-Sitzungsinformationen, um böswillige Bots besser erkennen zu können.

Weitere Informationen finden Sie unter [AWS WAF Regelgruppe „Bot-Kontrolle“](#) und [AWS WAF Bot-Steuerung](#).

Informationen zum Hinzufügen einer dieser verwalteten Regelgruppen zu Ihrer Web-ACL finden Sie in den Verfahren [Hinzufügen der verwalteten ACFP-Regelgruppe zu Ihrer Web-ACL](#), [Hinzufügen der von ATP verwalteten Regelgruppe zu Ihrer Web-ACL](#), und [Hinzufügen der von AWS WAF Bot Control verwalteten Regelgruppe zu Ihrer Web-ACL](#).

Note

Die verwalteten Regelgruppen blockieren derzeit keine Anfragen, denen Token fehlen. Um Anfragen zu blockieren, bei denen Token fehlen, folgen Sie nach der Implementierung Ihrer APIs für die Anwendungsintegration den Anweisungen unter [Anfragen blockieren, die kein gültiges Token haben](#).

Zugriff auf die Integrations-APIs

Die JavaScript Integrations-APIs sind allgemein verfügbar, und Sie können sie für Ihre Browser und andere Geräte verwenden, die ausgeführt werden JavaScript.

AWS WAF bietet benutzerdefinierte SDKs zur intelligenten Bedrohungsintegration für mobile Android- und iOS-Apps.

- Für mobile Android-Apps funktionieren die AWS WAF SDKs für die Android-API-Version 23 (Android-Version 6) und höher. Informationen zu Android-Versionen finden Sie in den [Versionshinweisen zur SDK-Plattform](#).
- Für mobile iOS-Apps funktionieren AWS WAF SDKs für iOS-Version 13 und höher. Informationen zu iOS-Versionen findest du in den [Versionshinweisen zu iOS und iPadOS](#).

So greifen Sie über die Konsole auf die Integrations-APIs zu

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich Anwendungsintegration und dann die Registerkarte aus, an der Sie interessiert sind.

- Die intelligente Bedrohungsintegration ist für JavaScript mobile Anwendungen verfügbar.

Die Registerkarte enthält Folgendes:

- Eine Liste der Web-ACLs, die für die Integration intelligenter Bedrohungsanwendungen aktiviert sind. Die Liste enthält jede Web-ACL, die die `AWSManagedRulesACFPRuleSet` verwaltete Regelgruppe, die `AWSManagedRulesATPRuleSet` verwaltete Regelgruppe oder die gezielte Schutzstufe der `AWSManagedRulesBotControlRuleSet` verwalteten Regelgruppe verwendet. Wenn Sie die APIs für intelligente Bedrohungen implementieren, verwenden Sie die Integrations-URL für die Web-ACL, in die Sie integrieren möchten.
- Die APIs, auf die Sie Zugriff haben. Die JavaScript APIs sind immer verfügbar. Für den Zugriff auf die mobilen SDKs wenden Sie sich an den Support unter [Kontakt AWS](#).
- Die CAPTCHA-Integration ist für Anwendungen verfügbar. JavaScript

Die Registerkarte enthält Folgendes:

- Die Integrations-URL zur Verwendung in Ihrer Integration.
- Die API-Schlüssel, die Sie für Ihre Client-Anwendungsdomänen erstellt haben. Ihre Verwendung der CAPTCHA-API erfordert einen verschlüsselten API-Schlüssel, der Kunden das Recht gibt, von ihren Domains aus auf AWS WAF CAPTCHA zuzugreifen. Verwenden Sie für jeden Client, mit dem Sie eine Integration durchführen, einen API-Schlüssel, der die Domain des Kunden enthält. Weitere Informationen zu diesen Anforderungen und zur Verwaltung dieser Schlüssel finden Sie unter [Verwaltung von API-Schlüsseln für die JS-CAPTCHA-API](#).

AWS WAF JavaScript Integrationen

Sie können die JavaScript Integrations-APIs verwenden, um AWS WAF Anwendungsintegrationen in Ihren Browsern und anderen Geräten zu implementieren, die ausgeführt JavaScript werden.

- Mit den APIs für intelligente Bedrohungen können Sie die Token-Autorisierung über eine automatische clientseitige Browser-Anfrage verwalten und die Token in die Anfragen aufnehmen, die Sie an Ihre geschützten Ressourcen senden.
- Die CAPTCHA-Integrations-API ergänzt die intelligenten Bedrohungs-APIs und ermöglicht es Ihnen, die Platzierung und die Eigenschaften des CAPTCHA-Puzzles in Ihren Client-Anwendungen anzupassen. Diese API nutzt die APIs für intelligente Bedrohungen, um AWS WAF Token für die Verwendung auf der Seite zu erwerben, nachdem der Endbenutzer das CAPTCHA-Puzzle erfolgreich gelöst hat.

Durch die Verwendung dieser Integrationen stellen Sie sicher, dass die Remote-Prozedur-Aufrufe Ihres Clients ein gültiges Token enthalten. Wenn diese Integrations-APIs auf den Seiten Ihrer Anwendung vorhanden sind, können Sie in Ihrer Web-ACL Regeln zur Risikominderung implementieren, wie z. B. das Blockieren von Anfragen, die kein gültiges Token enthalten. Sie können auch Regeln implementieren, die die Verwendung der Token, die Ihre Client-Anwendungen erhalten, erzwingen, indem Sie die CAPTCHA Aktionen Challenge oder in Ihren Regeln verwenden.

Die folgende Liste zeigt die grundlegenden Komponenten einer typischen Implementierung der Intelligent Threat APIs auf einer Webanwendungsseite.

```
<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>
```

Mit der CAPTCHA-Integrations-API können Sie das CAPTCHA-Puzzle-Erlebnis Ihrer Endbenutzer individuell anpassen. Die CAPTCHA-Integration nutzt die JavaScript intelligente Bedrohungsintegration für die Browserverifizierung und die Tokenverwaltung und fügt eine Funktion zur Konfiguration und Darstellung des CAPTCHA-Puzzles hinzu.

Die folgende Liste zeigt die grundlegenden Komponenten einer typischen Implementierung der JavaScript CAPTCHA-API auf einer Webanwendungsseite.

```
<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>
```

Themen

- [Bereitstellung von Domains zur Verwendung in den Tokens](#)
- [Verwenden der JavaScript API mit Inhaltssicherheitsrichtlinien](#)
- [Verwendung der Intelligent Threat JavaScript API](#)
- [Verwenden der CAPTCHA-API JavaScript](#)

Bereitstellung von Domains zur Verwendung in den Tokens

Beim Erstellen eines Tokens AWS WAF wird standardmäßig die Hostdomäne der Ressource verwendet, die der Web-ACL zugeordnet ist. Sie können zusätzliche Domänen für die Token bereitstellen, die für die JavaScript APIs AWS WAF erstellt werden. Konfigurieren Sie dazu die globale Variable `window.awsWafCookieDomainList` mit einer oder mehreren Tokendomänen.

Beim AWS WAF Erstellen eines Tokens wird aus der Kombination der Domänen in `window.awsWafCookieDomainList` und der Hostdomäne der Ressource, die der Web-ACL zugeordnet ist, die geeignetste, kürzeste Domain verwendet.

Beispieleinstellungen:

```
window.awsWafCookieDomainList = ['.aws.amazon.com']
```

```
window.awsWafCookieDomainList = ['.aws.amazon.com', 'abc.aws.amazon.com']
```

Sie können in dieser Liste keine öffentlichen Suffixe verwenden. Beispielsweise können Sie `gov . au` oder nicht `co . uk` als Tokendomänen in der Liste verwenden.

Die Domänen, die Sie in dieser Liste angeben, müssen mit Ihren anderen Domänen und Domänenkonfigurationen kompatibel sein:

- Bei den Domains muss es sich um solche handeln, die auf der geschützten Host-Domain und der Token-Domainliste basieren, die für die Web-ACL konfiguriert ist. AWS WAF Weitere Informationen finden Sie unter [Konfiguration der Domainliste für Web-ACL-Tokens](#).
- Wenn Sie die JavaScript CAPTCHA-API verwenden, muss mindestens eine Domain in Ihrem CAPTCHA-API-Schlüssel exakt mit einer der Token-Domains in übereinstimmen, `window.awsWafCookieDomainList` oder es muss sich um die Apex-Domain einer dieser Token-Domains handeln.

Für die Token-Domain `mySubdomain.myApex.com` stimmt der API-Schlüssel beispielsweise exakt überein und der API-Schlüssel `mySubdomain.myApex.com` entspricht der Apex-Domain. `myApex.com` Jeder Schlüssel entspricht der Token-Domain.

Weitere Informationen zu den API-Schlüsseln finden Sie unter [Verwaltung von API-Schlüsseln für die JS-CAPTCHA-API](#).

Wenn Sie die `AWSManagedRulesACFPRuleSet` verwaltete Regelgruppe verwenden, können Sie eine Domäne konfigurieren, die mit der Domäne im Kontoerstellungspfad übereinstimmt, den Sie für die Regelgruppenkonfiguration angegeben haben. Weitere Informationen zu dieser Konfiguration finden Sie unter [Hinzufügen der verwalteten ACFP-Regelgruppe zu Ihrer Web-ACL](#).

Wenn Sie die `AWSManagedRulesATPRuleSet` verwaltete Regelgruppe verwenden, können Sie eine Domäne konfigurieren, die mit der Domäne im Anmeldepfad übereinstimmt, die Sie für die Regelgruppenkonfiguration angegeben haben. Weitere Informationen zu dieser Konfiguration finden Sie unter [Hinzufügen der von ATP verwalteten Regelgruppe zu Ihrer Web-ACL](#).

Verwenden der JavaScript API mit Inhaltssicherheitsrichtlinien

Wenn Sie Inhaltssicherheitsrichtlinien (CSP) auf Ihre Ressourcen anwenden, müssen Sie die JavaScript AWS WAF Apex-Domain auf eine Zulassungsliste setzen, damit Ihre Implementierung funktioniert. `aws.waf.com` Die JavaScript SDKs rufen verschiedene AWS WAF Endpunkte auf, sodass für diese Domain die Berechtigungen bereitgestellt werden, die für den Betrieb der SDKs erforderlich sind.

Im Folgenden wird eine Beispielkonfiguration für die Zulassungsliste der Apex-Domain gezeigt: AWS WAF

```
connect-src 'self' https://*.aws.waf.com;  
script-src 'self' https://*.aws.waf.com;  
script-src-elem 'self' https://*.aws.waf.com;
```

Wenn Sie versuchen, die JavaScript SDKs mit Ressourcen zu verwenden, die CSP verwenden, und Sie die AWS WAF Domain nicht auf die Zulassungsliste gesetzt haben, erhalten Sie Fehlermeldungen wie die folgenden:

```
Refused to load the script ...aws.waf.com/<> because it violates the following Content  
Security Policy directive: "script-src 'self'"
```

Verwendung der Intelligent Threat JavaScript API

Die intelligenten Bedrohungs-APIs bieten Funktionen für die Ausführung von Anfragen im Hintergrund gegen den Browser des Benutzers und für die Verarbeitung von AWS WAF Tokens, die den Nachweis erfolgreicher Abfragen und CAPTCHA-Antworten liefern.

Implementieren Sie die JavaScript Integration zunächst in einer Testumgebung und dann in der Produktion. Weitere Anleitungen zur Codierung finden Sie in den folgenden Abschnitten.

Um die APIs für intelligente Bedrohungen zu verwenden

1. Installieren Sie die APIs

Wenn Sie die CAPTCHA-API verwenden, können Sie diesen Schritt überspringen. Wenn Sie die CAPTCHA-API installieren, installiert das Skript automatisch die APIs für intelligente Bedrohungen.

- a. [Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter https://console.aws.amazon.com/wafv2/.](https://console.aws.amazon.com/wafv2/)
- b. Wählen Sie im Navigationsbereich Application integration (Anwendungsintegration) aus. Auf der Seite zur Anwendungsintegration finden Sie Optionen in Registerkarten.
- c. Wählen Sie Intelligente Bedrohungsintegration
- d. Wählen Sie auf der Registerkarte die Web-ACL aus, in die Sie integrieren möchten. Die Web-ACL-Liste enthält nur Web-ACLs, die die `AWSManagedRulesACFPRuleSet` verwaltete Regelgruppe, die `AWSManagedRulesATPRuleSet` verwaltete Regelgruppe oder die gezielte Schutzstufe der `AWSManagedRulesBotControlRuleSet` verwalteten Regelgruppe verwenden.
- e. Öffnen Sie den JavaScript SDK-Bereich und kopieren Sie das Skript-Tag zur Verwendung in Ihrer Integration.
- f. Fügen Sie im Seitencode Ihrer Anwendung im `<head>` Abschnitt das Skript-Tag ein, das Sie für die Web-ACL kopiert haben. Diese Einbeziehung bewirkt, dass Ihre Clientanwendung beim Laden der Seite automatisch ein Token im Hintergrund abrufen.

```
<head>
  <script type="text/javascript" src="Web ACL integration URL/challenge.js"
    defer></script>
</head>
```

Diese `<script>`-Auflistung wird mit dem `defer`-Attribut konfiguriert, doch Sie können die Einstellung in `async` ändern, wenn sich die Seite auf andere Weise verhalten soll.

2. (Optional) Fügen Sie die Domänenkonfiguration für die Token des Clients hinzu — Standardmäßig AWS WAF wird beim Erstellen eines Tokens die Hostdomäne der Ressource verwendet, die der Web-ACL zugeordnet ist. Um zusätzliche Domänen für die JavaScript APIs bereitzustellen, folgen Sie den Anweisungen unter [Bereitstellung von Domains zur Verwendung in den Tokens](#).
3. Codieren Sie Ihre intelligente Bedrohungsintegration — Verfassen Sie Ihren Code, um sicherzustellen, dass der Token-Abruf abgeschlossen ist, bevor der Client seine Anfragen an Ihre geschützten Endgeräte sendet. Wenn Sie für den Aufruf bereits die `fetch`-API verwenden, können Sie den `fetch`-Wrapper der AWS WAF -Integration ersetzen. Wenn Sie die `fetch` API nicht verwenden, können Sie stattdessen den `AWS WAF getToken` Integrationsvorgang verwenden. In den folgenden Abschnitten finden Sie weitere Code-Anweisungen.

4. Fügen Sie Ihrer Web-ACL eine Token-Verifizierung hinzu — Fügen Sie Ihrer Web-ACL mindestens eine Regel hinzu, die prüft, ob in den von Ihrem Client gesendeten Webanfragen ein gültiges Challenge-Token vorhanden ist. Sie können Regelgruppen verwenden, die Challenge-Token überprüfen und überwachen, z. B. die Zielebene der verwalteten Regelgruppe von Bot Control, und Sie können die Challenge Regelaktion zur Überprüfung verwenden, wie unter [beschrieben CAPTCHA und Challenge in AWS WAF](#).

Die Web-ACL-Ergänzungen überprüfen, ob Anfragen an Ihre geschützten Endgeräte das Token enthalten, das Sie in Ihrer Client-Integration erworben haben. Anfragen, die ein gültiges, noch nicht abgelaufenes Token enthalten, bestehen die Challenge Prüfung und senden keine weitere stille Aufforderung an Ihren Kunden.

5. (Optional) Blockieren Sie Anfragen, bei denen Token fehlen — Wenn Sie die APIs mit der verwalteten ACFP-Regelgruppe, der von ATP verwalteten Regelgruppe oder den gezielten Regeln der Bot-Control-Regelgruppe verwenden, blockieren diese Regeln keine Anfragen, bei denen Token fehlen. Folgen Sie den Anweisungen unter, um Anfragen zu blockieren, bei [Anfragen blockieren, die kein gültiges Token haben](#) denen Token fehlen.

Themen

- [API-Spezifikation für intelligente Bedrohungen](#)
- [Wie benutzt man den Integration fetch Wrapper](#)
- [Wie benutzt man die Integration getToken](#)

API-Spezifikation für intelligente Bedrohungen

In diesem Abschnitt werden die Spezifikationen für die Methoden und Eigenschaften der APIs zur intelligenten Bedrohungsabwehr JavaScript aufgeführt. Verwenden Sie diese APIs für intelligente Bedrohungs- und CAPTCHA-Integrationen.

AwsWafIntegration.fetch()

Sendet die fetch HTTP-Anfrage mithilfe der Integrationsimplementierung an den AWS WAF Server.

AwsWafIntegration.getToken()

Ruft das gespeicherte AWS WAF Token ab und speichert es in einem Cookie auf der aktuellen Seite mit dem Namen und dem Wert `aws-waf-token`, der auf den Tokenwert gesetzt ist.

AwsWafIntegration.hasToken()

Gibt einen booleschen Wert zurück, der angibt, ob das `aws-waf-token` Cookie derzeit ein nicht abgelaufenes Token enthält.

Wenn Sie auch die CAPTCHA-Integration verwenden, finden Sie die entsprechende Spezifikation unter [JavaScript CAPTCHA-API-Spezifikation](#)

Wie benutzt man den Integration **fetch** Wrapper

Sie verwenden den AWS WAF `fetch`-Wrapper, indem Sie Ihre regulären `fetch`-Aufrufe in die `fetch`-API unter dem `AwsWafIntegration`-Namespace ändern. Der AWS WAF Wrapper unterstützt dieselben Optionen wie der JavaScript `fetch` Standard-API-Aufruf und fügt die Token-Behandlung für die Integration hinzu. Dieser Ansatz ist im Allgemeinen die einfachste Möglichkeit, Ihre Anwendung zu integrieren.

Vor der Wrapper-Implementierung

Die folgende Beispielliste zeigt Standardcode vor der Implementierung des `AwsWafIntegration-fetch`-Wrapper.

```
const login_response = await fetch(login_url, {
  method: 'POST',
  headers: {
    'Content-Type': 'application/json'
  },
  body: login_body
});
```

Nach der Wrapper-Implementierung

Die folgende Auflistung zeigt den gleichen Code wie bei der Implementierung des `AwsWafIntegration-fetch`-Wrapper.

```
const login_response = await AwsWafIntegration.fetch(login_url, {
  method: 'POST',
  headers: {
    'Content-Type': 'application/json'
  },
  body: login_body
});
```

Wie benutzt man die Integration **getToken**

AWS WAF erfordert, dass Ihre Anfragen an geschützte Endpunkte das Cookie enthalten, das `aws-waf-token` mit dem Wert Ihres aktuellen Tokens benannt ist.

Bei der `getToken` Operation handelt es sich um einen asynchronen API-Aufruf, der das AWS WAF Token abrufen und es in einem Cookie auf der aktuellen Seite speichert `aws-waf-token`, wobei der Name und der Wert auf den Tokenwert gesetzt sind. Sie können dieses Token-Cookie nach Bedarf auf Ihrer Seite verwenden.

Wenn Sie `getToken` aufrufen, geschieht Folgendes:

- Wenn ein nicht abgelaufenes Token bereits verfügbar ist, gibt der Aufruf es sofort zurück.
- Andernfalls wird ein neues Token aus dem -Token-Anbieter aufgerufen. Wird der Workflow für den Token-Erwerb nicht innerhalb von 2 Sekunden abgeschlossen, tritt eine Zeitüberschreitung ein. Wenn die Zeitüberschreitung eingetreten ist, wird ein Fehler ausgelöst, der von Ihrem Aufrufcode behoben werden muss.

Der `getToken`-Betrieb verfügt über den begleitenden `hasToken`-Betrieb, der angibt, ob das `aws-waf-token`-Cookie derzeit ein nicht abgelaufenes Token enthält.

`AwsWafIntegration.getToken()` ruft ein gültiges Token ab und speichert es als Cookie. Bei den meisten Client-Aufrufen wird dieses Cookie automatisch angehängt, bei einigen jedoch nicht. Bei Aufrufen über Host-Domains hinweg wird das Cookie beispielsweise nicht angehängt. In den folgenden Implementierungsdetails zeigen wir, wie Sie mit beiden Arten von Client-Aufrufen arbeiten können.

Grundlegende **getToken** Implementierung für Aufrufe, die das **aws-waf-token** Cookie anhängen

Die folgende Beispielliste zeigt Standardcode für die Implementierung des `getToken` Vorgangs mit einer Anmeldeanforderung.

```
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
}
```

Senden Sie das Formular erst ab, wenn das Token unter **getToken** verfügbar ist.

Die folgende Auflistung zeigt, wie Sie einen Ereignis-Listener registrieren, um Formularübermittlungen abzufangen, bis ein gültiges Token zur Verwendung verfügbar ist.

```
<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>
```

Anhängen des Tokens, wenn Ihr Client das **aws-waf-token** Cookie nicht standardmäßig anhängt

`AwsWafIntegration.getToken()` ruft ein gültiges Token ab und speichert es als Cookie, aber nicht alle Client-Aufrufe hängen dieses Cookie standardmäßig an. Beispielsweise hängen Aufrufe über Hostdomänen hinweg das Cookie nicht an.

Der `fetch` Wrapper behandelt diese Fälle automatisch, aber wenn Sie den `fetch` Wrapper nicht verwenden können, können Sie dies mithilfe eines benutzerdefinierten `x-aws-waf-token` Headers handhaben. AWS WAF liest Token aus diesem Header und liest sie zusätzlich aus dem `aws-waf-token` Cookie. Der folgende Code zeigt ein Beispiel für das Setzen des Headers.

```
const token = await AwsWafIntegration.getToken();
const result = await fetch('/url', {
  headers: {
    'x-aws-waf-token': token,
  },
});
```

Akzeptiert standardmäßig AWS WAF nur Token, die dieselbe Domain wie die angeforderte Host-Domain enthalten. Für alle domänenübergreifenden Token sind entsprechende Einträge in der Domainliste der Web-ACL-Tokens erforderlich. Weitere Informationen finden Sie unter [Konfiguration der Domainliste für Web-ACL-Tokens](#).

Weitere Informationen zur domänenübergreifenden Verwendung von Token finden Sie unter [aws-waf-bot-controlaws-samples/](#) - `api-protection-with-captcha`

Verwenden der CAPTCHA-API JavaScript

Mit der JavaScript CAPTCHA-API können Sie das CAPTCHA-Puzzle konfigurieren und an der gewünschten Stelle in Ihrer Client-Anwendung platzieren. Diese API nutzt die Funktionen der JavaScript APIs für intelligente Bedrohungen, um AWS WAF Token zu erwerben und zu verwenden, nachdem ein Endbenutzer ein CAPTCHA-Puzzle erfolgreich gelöst hat.

Implementieren Sie die JavaScript Integration zunächst in einer Testumgebung und dann in der Produktion. Weitere Anleitungen zur Codierung finden Sie in den folgenden Abschnitten.

Um die CAPTCHA-Integrations-API zu verwenden

1. Installieren Sie die API
 - a. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
 - b. Wählen Sie im Navigationsbereich Application integration (Anwendungsintegration) aus. Auf der Seite zur Anwendungsintegration finden Sie Optionen in Registerkarten.
 - c. Wählen Sie CAPTCHA-Integration aus.

- d. Kopieren Sie das aufgelistete JavaScript Integrationskript-Tag zur Verwendung in Ihrer Integration.
- e. Fügen Sie im Code Ihrer Anwendungsseite im <head> Abschnitt das Skript-Tag ein, das Sie kopiert haben. Durch diese Aufnahme steht das CAPTCHA-Puzzle zur Konfiguration und Verwendung zur Verfügung.

```
<head>
  <script type="text/javascript" src="integrationURL/jsapi.js" defer></
script>
</head>
```

Diese <script>-Auflistung wird mit dem `defer`-Attribut konfiguriert, doch Sie können die Einstellung in `async` ändern, wenn sich die Seite auf andere Weise verhalten soll.

Das CAPTCHA-Skript lädt auch automatisch das intelligente Threat-Integrationskript, falls es noch nicht vorhanden ist. Das Skript zur intelligenten Bedrohungsintegration veranlasst Ihre Client-Anwendung, beim Laden der Seite automatisch ein Token im Hintergrund abzurufen, und bietet weitere Funktionen zur Tokenverwaltung, die Sie für die Verwendung der CAPTCHA-API benötigen.

2. (Optional) Fügen Sie die Domänenkonfiguration für die Token des Clients hinzu — Standardmäßig AWS WAF wird bei der Erstellung eines Tokens die Hostdomäne der Ressource verwendet, die der Web-ACL zugeordnet ist. Um zusätzliche Domänen für die JavaScript APIs bereitzustellen, folgen Sie den Anweisungen unter [Bereitstellung von Domains zur Verwendung in den Tokens](#).
3. Holen Sie sich den verschlüsselten API-Schlüssel für den Client — Die CAPTCHA-API benötigt einen verschlüsselten API-Schlüssel, der eine Liste gültiger Client-Domains enthält. AWS WAF verwendet diesen Schlüssel, um zu überprüfen, ob die Client-Domain, die Sie mit der Integration verwenden, für die Verwendung AWS WAF von CAPTCHA zugelassen ist. Folgen Sie den Anweisungen unter, um Ihren API-Schlüssel zu generieren. [Verwaltung von API-Schlüsseln für die JS-CAPTCHA-API](#)
4. Codieren Sie Ihre CAPTCHA-Widget-Implementierung — Implementieren Sie den `renderCaptcha()` API-Aufruf auf Ihrer Seite an der Stelle, an der Sie ihn verwenden möchten. Informationen zur Konfiguration und Verwendung dieser Funktion finden Sie in den folgenden Abschnitten und. [JavaScript CAPTCHA-API-Spezifikation](#) [Wie rendert man das CAPTCHA-Puzzle](#)

Die CAPTCHA-Implementierung ist in die intelligenten Threat-Integrations-APIs für die Tokenverwaltung und die Ausführung von Abruf-Aufrufen integriert, die die Token verwenden. AWS WAF Hinweise zur Verwendung dieser APIs finden Sie unter. [Verwendung der Intelligent Threat JavaScript API](#)

5. Fügen Sie Ihrer Web-ACL eine Token-Verifizierung hinzu — Fügen Sie Ihrer Web-ACL mindestens eine Regel hinzu, die überprüft, ob in den von Ihrem Client gesendeten Webanfragen ein gültiges CAPTCHA-Token vorhanden ist. Sie können die CAPTCHA Regelaktion zur Überprüfung verwenden, wie unter beschrieben. [CAPTCHA und Challenge in AWS WAF](#)

Die Web-ACL-Ergänzungen überprüfen, ob Anfragen, die an Ihre geschützten Endgeräte gesendet werden, das Token enthalten, das Sie in Ihrer Client-Integration erworben haben. Anfragen, die ein gültiges, noch nicht abgelaufenes CAPTCHA-Token enthalten, bestehen die Prüfung der CAPTCHA Regelaktion und stellen Ihren Endbenutzer nicht vor ein weiteres CAPTCHA-Puzzle.

Themen

- [JavaScript CAPTCHA-API-Spezifikation](#)
- [Wie rendert man das CAPTCHA-Puzzle](#)
- [Umgang mit einer CAPTCHA-Antwort von AWS WAF](#)
- [Verwaltung von API-Schlüsseln für die JS-CAPTCHA-API](#)

JavaScript CAPTCHA-API-Spezifikation

In diesem Abschnitt werden die Spezifikationen für die Methoden und Eigenschaften der JavaScript CAPTCHA-APIs aufgeführt. Verwenden Sie die JavaScript CAPTCHA-APIs, um benutzerdefinierte CAPTCHA-Rätsel in Ihren Client-Anwendungen auszuführen.

Diese API baut auf den intelligenten Bedrohungs-APIs auf, mit denen Sie die Erfassung und Verwendung von AWS WAF Token konfigurieren und verwalten. Siehe [API-Spezifikation für intelligente Bedrohungen](#).

AwsWafCaptcha.renderCaptcha(container, configuration)

Präsentiert dem Endbenutzer ein AWS WAF CAPTCHA-Puzzle und aktualisiert bei Erfolg das Client-Token mit der CAPTCHA-Validierung. Dies ist nur mit der CAPTCHA-Integration verfügbar. Verwenden Sie diesen Aufruf zusammen mit den intelligenten Bedrohungs-APIs, um

den Token-Abruf zu verwalten und das Token in Ihren Aufrufen bereitzustellen. `fetch` Die APIs für intelligente Bedrohungen finden Sie unter [API-Spezifikation für intelligente Bedrohungen](#).

Im Gegensatz zum CAPTCHA-Interstitial, das AWS WAF gesendet wird, zeigt das mit dieser Methode gerenderte CAPTCHA-Puzzle das Rätsel sofort an, ohne dass ein anfänglicher Titelbildschirm angezeigt wird.

container

Das Element Objekt für das Zielcontainerelement auf der Seite. Dies wird üblicherweise durch Aufrufen von `document.getElementById()` oder `abgerufendocument.querySelector()`.

Erforderlich: Ja

Typ: Element

Konfiguration

Ein Objekt, das CAPTCHA-Konfigurationseinstellungen wie folgt enthält:

apiKey

Der verschlüsselte API-Schlüssel, der Berechtigungen für die Domäne des Kunden aktiviert. Verwenden Sie die AWS WAF Konsole, um Ihre API-Schlüssel für Ihre Kundendomänen zu generieren. Sie können einen Schlüssel für bis zu fünf Domains verwenden. Weitere Informationen finden Sie unter [Verwaltung von API-Schlüsseln für die JS-CAPTCHA-API](#).

Erforderlich: Ja

Typ: string

onSuccess: (wafToken: string) => void;

Wird mit einem gültigen AWS WAF Token aufgerufen, wenn der Endbenutzer ein CAPTCHA-Rätsel erfolgreich gelöst hat. Verwenden Sie das Token in den Anfragen, die Sie an die Endgeräte senden, die Sie mit einer AWS WAF Web-ACL schützen. Das Token liefert den Nachweis und den Zeitstempel für die letzte erfolgreiche Lösung des Rätsels.

Erforderlich: Ja

onError?: (error: CaptchaError) => void;

Wird mit einem Fehlerobjekt aufgerufen, wenn während der CAPTCHA-Operation ein Fehler auftritt.

Erforderlich: Nein

CaptchaErrorKlassendefinition — Der `onError` Handler liefert einen Fehlertyp mit der folgenden Klassendefinition.

```
CaptchaError extends Error {  
  kind: "internal_error" | "network_error" | "token_error" | "client_error";  
  statusCode?: number;  
}
```

- `kind`— Die Art des zurückgegebenen Fehlers.
- `statusCode`— Der HTTP-Statuscode, falls verfügbar. Dieser wird verwendet, `network_error` wenn der Fehler auf einen HTTP-Fehler zurückzuführen ist.

onLoad?: () => void;

Wird aufgerufen, wenn ein neues CAPTCHA-Rätsel geladen wird.

Erforderlich: Nein

onPuzzleTimeout?: () => void;

Wird aufgerufen, wenn ein CAPTCHA-Rätsel nicht gelöst wird, bevor es abläuft.

Erforderlich: Nein

onPuzzleCorrect?: () => void;

Wird aufgerufen, wenn eine richtige Antwort auf ein CAPTCHA-Rätsel gegeben wurde.

Erforderlich: Nein

onPuzzleIncorrect?: () => void;

Wird aufgerufen, wenn eine falsche Antwort auf ein CAPTCHA-Rätsel gegeben wird.

Erforderlich: Nein

defaultLocale

Das Standard-Gebietsschema, das für das CAPTCHA-Rätsel verwendet werden soll. Die schriftlichen Anweisungen für CAPTCHA-Rätsel sind in Arabisch (ar-SA), vereinfachtem Chinesisch (zh-CN), Niederländisch (nl-NL), Englisch (en-US), Französisch (fr-FR), Deutsch (de-DE), Italienisch (it-IT), Japanisch (ja-JP), Portugiesisch (pt-BR), Spanisch (es-ES) und Türkisch (tr-TR) verfügbar. Audioanweisungen sind für alle Schriftsprachen

verfügbar, mit Ausnahme von Chinesisch und Japanisch, für die standardmäßig Englisch verwendet wird. Um die Standardsprache zu ändern, geben Sie die internationale Sprache und den Ländercode an, `ar-SA` z. B.

Standard: Die Sprache, die derzeit im Browser des Endbenutzers verwendet wird

Erforderlich: Nein

Typ: `string`

`disableLanguageSelector`

Wenn auf `gesetzt true`, verbirgt das CAPTCHA-Puzzle die Sprachauswahl.

Standard: `false`

Erforderlich: Nein

Typ: `boolean`

`dynamicWidth`

Wenn auf `gesetzt true`, ändert das CAPTCHA-Puzzle aus Gründen der Kompatibilität mit der Breite des Browserfensters seine Breite.

Standard: `false`

Erforderlich: Nein

Typ: `boolean`

`skipTitle`

Wenn diese Option auf `gesetzt ist true`, zeigt das CAPTCHA-Puzzle nicht die Überschrift Löse das Rätsel an.

Standard: `false`

Erforderlich: Nein

Typ: `boolean`

Wie rendert man das CAPTCHA-Puzzle

Sie können den AWS WAF `renderCaptcha` Anruf an der gewünschten Stelle in Ihrer Client-Oberfläche verwenden. Der Aufruf ruft ein CAPTCHA-Puzzle ab AWS WAF, rendert es und

sendet die Ergebnisse zur Überprüfung an. AWS WAF Wenn Sie den Aufruf tätigen, geben Sie die Konfiguration für das Rendern von Rätseln und die Callbacks an, die Sie ausführen möchten, wenn Ihre Endbenutzer das Rätsel gelöst haben. Einzelheiten zu den Optionen finden Sie im vorherigen Abschnitt, [JavaScript CAPTCHA-API-Spezifikation](#).

Verwenden Sie diesen Aufruf in Verbindung mit der Token-Management-Funktionalität der Intelligent Threat Integration APIs. Durch diesen Aufruf erhält Ihr Kunde ein Token, das den erfolgreichen Abschluss des CAPTCHA-Rätsels bestätigt. Verwenden Sie die intelligenten APIs zur Integration von Bedrohungen, um das Token zu verwalten und das Token in den Aufrufen Ihres Kunden an die Endgeräte bereitzustellen, die mit Web-ACLs geschützt sind. AWS WAF Informationen zu den APIs für intelligente Bedrohungen finden Sie unter [Verwendung der Intelligent Threat JavaScript API](#)

Beispiel für eine Implementierung

Die folgende Beispielliste zeigt eine standardmäßige CAPTCHA-Implementierung, einschließlich der Platzierung der AWS WAF Integrations-URL im <head> Abschnitt.

In dieser Auflistung wird die `renderCaptcha` Funktion mit einem erfolgreichen Callback konfiguriert, der den `AwsWafIntegration.fetch` Wrapper der Intelligent Threat Integration APIs verwendet. Hinweise zu dieser Funktion finden Sie unter [Wie benutzt man den Integration fetch Wrapper](#)

```
<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>

```

Beispiel für Konfigurationseinstellungen

Die folgende Beispielliste zeigt die Optionen `renderCaptcha` mit nicht standardmäßigen Einstellungen für die Breite und den Titel.

```

AwsWafCaptcha.renderCaptcha(container, {
  apiKey: "...API key goes here...",
  onSuccess: captchaExampleSuccessFunction,
  onError: captchaExampleErrorFunction,
  dynamicWidth: true,
  skipTitle: true
});

```

Vollständige Informationen zu den Konfigurationsoptionen finden Sie unter [JavaScript CAPTCHA-API-Spezifikation](#).

Umgang mit einer CAPTCHA-Antwort von AWS WAF

Eine AWS WAF Regel mit einer CAPTCHA Aktion beendet die Auswertung einer passenden Webanfrage, wenn die Anfrage kein Token mit einem gültigen CAPTCHA-Zeitstempel enthält. Handelt es sich bei der Anfrage um einen GET Text-/HTML-Aufruf, stellt die CAPTCHA Aktion dem

Client dann ein Interstitial mit einem CAPTCHA-Rätsel zur Verfügung. Wenn Sie die JavaScript CAPTCHA-API nicht integrieren, führt das Interstitial das Rätsel aus, und wenn der Endbenutzer es erfolgreich löst, wird die Anfrage automatisch erneut gesendet.

Wenn Sie die JavaScript CAPTCHA-API integrieren und Ihre CAPTCHA-Handhabung anpassen, müssen Sie die abschließende CAPTCHA-Antwort erkennen, Ihr benutzerdefiniertes CAPTCHA bereitstellen und dann, wenn der Endbenutzer das Rätsel erfolgreich löst, die Webanfrage des Kunden erneut einreichen.

Das folgende Codebeispiel veranschaulicht, wie dazu vorgegangen wird.

Note

Die AWS WAF CAPTCHA Aktionsantwort hat den Statuscode HTTP 405, anhand dessen wir die Antwort in diesem Code erkennen. CAPTCHA Wenn Ihr geschützter Endpunkt einen HTTP 405-Statuscode verwendet, um eine andere Art von Antwort für denselben Anruf zu übermitteln, wird mit diesem Beispielcode auch für diese Antworten ein CAPTCHA-Rätsel erstellt.

```
<!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>
```

Verwaltung von API-Schlüsseln für die JS-CAPTCHA-API

Um AWS WAF CAPTCHA mit der JavaScript API in eine Client-Anwendung zu integrieren, benötigen Sie das API-Integrations-Tag und den verschlüsselten JavaScript API-Schlüssel für die Client-Domain, auf der Sie Ihr CAPTCHA-Puzzle ausführen möchten.

Die CAPTCHA-Anwendungsintegration für JavaScript verwendet die verschlüsselten API-Schlüssel, um zu überprüfen, ob die Domäne der Client-Anwendung berechtigt ist, die CAPTCHA-API zu verwenden. AWS WAF Wenn Sie die CAPTCHA-API von Ihrem JavaScript Client aus aufrufen, geben Sie einen API-Schlüssel mit einer Domainliste an, die eine Domain für den aktuellen Client enthält. Sie können bis zu 5 Domains in einem einzigen verschlüsselten Schlüssel auflisten.

Anforderungen an API-Schlüssel

Der API-Schlüssel, den Sie in Ihrer CAPTCHA-Integration verwenden, muss eine Domain enthalten, die für den Client gilt, auf dem Sie den Schlüssel verwenden.

- Wenn Sie `window.awsWafCookieDomainList` in der intelligenten Bedrohungsintegration Ihres Kunden angeben, muss mindestens eine Domain in Ihrem API-Schlüssel exakt mit einer der Token-Domains in `window.awsWafCookieDomainList` übereinstimmen oder es muss sich um die Apex-Domain einer dieser Token-Domains handeln.

Für die Token-Domain `mySubdomain.myApex.com` entspricht der API-Schlüssel `mySubdomain.myApex.com` beispielsweise exakt und der API-Schlüssel `myApex.com` der Apex-Domain. Jeder Schlüssel entspricht der Token-Domain.

Hinweise zur Einstellung der Tokendomänenliste finden Sie unter [Bereitstellung von Domains zur Verwendung in den Tokens](#).

- Andernfalls muss die aktuelle Domain im API-Schlüssel enthalten sein. Die aktuelle Domain ist die Domain, die Sie in der Adressleiste des Browsers sehen können.

Basierend auf der geschützten Host-Domain und der Token-Domainliste, die für die Web-ACL konfiguriert ist, müssen die verwendeten Domains akzeptiert werden. AWS WAF Weitere Informationen finden Sie unter [Konfiguration der Domainliste für Web-ACL-Tokens](#).

Wie wählen Sie die Region für Ihren API-Schlüssel

AWS WAF kann CAPTCHA-API-Schlüssel in jeder Region generieren, in der sie verfügbar sind.

In der Regel sollten Sie für Ihren CAPTCHA-API-Schlüssel dieselbe Region verwenden wie für Ihre Web-ACL. Wenn Sie jedoch eine globale Zielgruppe für eine regionale Web-ACL erwarten, können Sie ein JavaScript CAPTCHA-Integrations-Tag für den Geltungsbereich CloudFront und einen API-Schlüssel für den Geltungsbereich abrufen und diese zusammen mit einer regionalen Web-ACL verwenden. CloudFront Dieser Ansatz ermöglicht es Kunden, ein CAPTCHA-Puzzle aus der Region zu laden, die ihnen am nächsten ist, wodurch die Latenz reduziert wird.

CAPTCHA-API-Schlüssel, die auf andere Regionen beschränkt sind, werden nicht für die Verwendung in CloudFront mehreren Regionen unterstützt. Sie können nur in der Region verwendet werden, auf die sie beschränkt sind.

Um einen API-Schlüssel für Ihre Kundendomänen zu generieren

Um die Integrations-URL abzurufen und die API-Schlüssel über die Konsole zu generieren und abzurufen.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich Application integration (Anwendungsintegration) aus.
3. Wählen Sie im Bereich Web-ACLs, die für die Anwendungsintegration aktiviert sind, die Region aus, die Sie für Ihren API-Schlüssel verwenden möchten. Sie können die Region auch im Bereich API-Schlüssel der Registerkarte CAPTCHA-Integration auswählen.
4. Wählen Sie den Tab CAPTCHA-Integration. Auf dieser Registerkarte finden Sie das JavaScript CAPTCHA-Integrations-Tag, das Sie in Ihrer Integration verwenden können, sowie die Liste der API-Schlüssel. Beide sind auf die ausgewählte Region beschränkt.
5. Wählen Sie im Bereich API-Schlüssel die Option Schlüssel generieren aus. Der Dialog zur Schlüsselgenerierung wird angezeigt.
6. Geben Sie die Client-Domänen ein, die Sie in den Schlüssel aufnehmen möchten. Sie können bis zu 5 eingeben. Wenn Sie fertig sind, wählen Sie Schlüssel generieren. Die Benutzeroberfläche kehrt zur Registerkarte CAPTCHA-Integration zurück, auf der Ihr neuer Schlüssel aufgeführt ist.

Einmal erstellt, ist ein API-Schlüssel unveränderlich. Wenn Sie Änderungen an einem Schlüssel vornehmen müssen, generieren Sie einen neuen Schlüssel und verwenden Sie ihn stattdessen.

7. (Optional) Kopieren Sie den neu generierten Schlüssel zur Verwendung in Ihrer Integration.

Sie können für diese Arbeit auch die REST-APIs oder eines der sprachspezifischen AWS SDKs verwenden. [Die REST-API-Aufrufe sind CreateApiKey und ListApiKeys.](#)

Um einen API-Schlüssel zu löschen

Um einen API-Schlüssel zu löschen, müssen Sie die REST-API oder eines der sprachspezifischen AWS SDKs verwenden. Der REST-API-Aufruf lautet [deleteAPIKey](#). Sie können die Konsole nicht verwenden, um einen Schlüssel zu löschen.

Nachdem Sie einen Schlüssel gelöscht haben, kann es bis zu 24 Stunden dauern, AWS WAF bis die Verwendung des Schlüssels in allen Regionen nicht mehr zulässig ist.


AWS WAF Integration mobiler Anwendungen

Sie können die AWS WAF mobilen SDKs verwenden, um AWS WAF intelligente Bedrohungsintegrations-SDKs für mobile Android- und iOS-Anwendungen zu implementieren.

- Für mobile Android-Apps funktionieren die AWS WAF SDKs für die Android-API-Version 23 (Android-Version 6) und höher. Informationen zu Android-Versionen finden Sie in den [Versionshinweisen zur SDK-Plattform](#).
- Für mobile iOS-Apps funktionieren AWS WAF SDKs für iOS-Version 13 und höher. Informationen zu iOS-Versionen findest du in den [Versionshinweisen zu iOS und iPadOS](#).

Das SDK für Mobilgeräte ermöglicht es Ihnen, die Token-Autorisierung zu verwalten und die Token in die Anforderungen aufzunehmen, die Sie an Ihre geschützten Ressourcen senden. Durch die Verwendung der SDKs stellen Sie sicher, dass diese Remote-Prozedur-Aufrufe durch Ihren Client ein gültiges Token enthalten. Wenn diese Integration auf den Seiten Ihrer Anwendung stattfindet, können Sie außerdem Risiko-reduzierende Regeln in Ihrer Web-ACL implementieren, z. B. das Blockieren von Anforderungen, die kein gültiges Token enthalten.

[Für den Zugriff auf die mobilen SDKs wenden Sie sich an den Support unter Kontakt. AWS](#)

 Note

Die AWS WAF mobilen SDKs sind nicht für die CAPTCHA-Anpassung verfügbar.

Der grundlegende Ansatz für die Verwendung des SDK besteht darin, mithilfe eines Konfigurationsobjekts einen Token-Anbieter zu erstellen und dann den Token-Anbieter zum Abrufen von Tokens zu verwenden. AWS WAF Standardmäßig schließt der Token-Anbieter die abgerufenen Token in die Webanforderungen an Ihre geschützte Ressource ein.

Im Folgenden finden Sie eine unvollständige Auflistung einer SDK-Implementierung, die die Hauptkomponenten zeigt. Weitere detaillierte Beispiele finden Sie unter [Schreiben Sie Ihren Code für das AWS WAF mobile SDK](#).

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();
```

Installation des SDK AWS WAF für Mobilgeräte

Um Zugriff auf die mobilen SDKs zu erhalten, wenden Sie sich an den Support unter [Kontakt AWS](#).

Implementieren Sie das SDK für Mobilgeräte zuerst in einer Testumgebung und dann in der Produktion.

Um das SDK für AWS WAF Mobilgeräte zu installieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich Application integration (Anwendungsintegration) aus.
3. Gehen Sie auf der Registerkarte Intelligente Bedrohungsintegrationen wie folgt vor:
 - a. Suchen Sie im Bereich Web ACLs that are enabled for application integration (Web-ACLs, die für die Anwendungsintegration aktiviert sind) nach der Web-ACL, in die Sie integrieren. Kopieren und speichern Sie die URL der Web-ACL-Integration zur Verwendung in Ihrer Implementierung. Sie können diese URL auch über den API-Aufruf GetWebACL abrufen.
 - b. Wählen Sie den Typ und die Version des Mobilgeräts und dann die Option Download (Herunterladen) aus. Sie können eine beliebige Version wählen, wir empfehlen jedoch, die neueste Version zu verwenden. AWS WAF lädt die zip Datei für Ihr Gerät an Ihren Standard-Download-Speicherort herunter.
4. Entpacken Sie die Datei in Ihrer App-Entwicklungsumgebung an einem Speicherort Ihrer Wahl. Suchen und öffnen Sie im Verzeichnis der ZIP-Datei die README-Datei. Folgen Sie den Anweisungen in der README Datei, um das AWS WAF mobile SDK zur Verwendung in Ihrem mobilen App-Code zu installieren.
5. Programmieren Sie Ihre App gemäß den Anweisungen in den folgenden Abschnitten.

Die AWS WAF mobile SDK-Spezifikation

In diesem Abschnitt werden die SDK-Objekte, -Operationen und -Konfigurationseinstellungen für die neueste verfügbare Version des SDK für AWS WAF Mobilgeräte aufgeführt. Ausführliche Informationen darüber, wie der Token-Anbieter und die Operationen für die verschiedenen Kombinationen von Konfigurationseinstellungen funktionieren, finden Sie unter [So funktioniert das SDK AWS WAF für Mobilgeräte](#).

WAFToken

Enthält ein AWS WAF Token.

getValue()

Ruft die String-Darstellung des WAFToken auf.

WAFTokenProvider

Verwaltet Token in Ihrer mobilen App. Implementieren Sie dies mit einem WAFConfiguration-Objekt.

getToken()

Wenn die Hintergrundaktualisierung aktiviert ist, wird das zwischengespeicherte Token zurückgegeben. Wenn die Aktualisierung im Hintergrund deaktiviert ist, wird ein synchroner, blockierender Aufruf AWS WAF zum Abrufen eines neuen Tokens ausgeführt.

onTokenReady(WAFTokenResultCallback)

Dadurch wird der Token-Anbieter angewiesen, das Token zu aktualisieren und das bereitgestellte Callback aufzurufen, wenn ein aktives Token bereit ist. Der Token-Anbieter ruft das Callback in einem Hintergrund-Thread auf, wenn das Token zwischengespeichert und bereit ist. Rufen Sie dies auf, wenn Ihre App zum ersten Mal geladen wird und wenn sie wieder in einen aktiven Zustand zurückversetzt wird. Weitere Informationen zum Zurückversetzen in einen aktiven Zustand finden Sie unter [the section called "Abrufen eines Tokens nach App-Inaktivität"](#).

Für Android- oder iOS-Apps können Sie WAFTokenResultCallback auf die Operation festlegen, die der Token-Anbieter ausführen soll, wenn ein angefordertes Token bereit ist. Bei Ihrer Implementierung von WAFTokenResultCallback müssen die Parameter WAFToken und SdkError übernommen werden. Für iOS-Apps können Sie alternativ eine Inline-Funktion erstellen.

storeTokenInCookieStorage(WAFToken)

Weist den `WAFTokenProvider` an, das angegebene AWS WAF Token im Cookie-Manager des SDK zu speichern. Standardmäßig wird das Token dem Cookie-Speicher nur hinzugefügt, wenn es zum ersten Mal abgerufen und aktualisiert wird. Wenn die Anwendung den gemeinsamen Cookie-Speicher aus irgendeinem Grund löscht, fügt das SDK das AWS WAF Token erst bei der nächsten Aktualisierung automatisch wieder hinzu.

WAFConfiguration

Enthält die Konfiguration für die Implementierung des `WAFTokenProvider`. Wenn Sie dies implementieren, geben Sie die Integrations-URL Ihrer Web-ACL, den Domainnamen, der im Token verwendet werden soll, und alle nicht standardmäßigen Einstellungen an, die der Token-Anbieter verwenden soll.

In der folgenden Liste sind die Konfigurationseinstellungen aufgeführt, die Sie im `WAFConfiguration`-Objekt verwalten.

applicationIntegrationUrl

Die URL der Anwendungsintegration. Rufen Sie dies von der AWS WAF Konsole oder über den `getWebACL` API-Aufruf ab.

Erforderlich: Ja

Typ: App-spezifische URL. Informationen zu iOS finden Sie unter [iOS URL](#) (iOS-URL). Informationen zu Android finden Sie unter [java.net URL](#) (java.net-URL).

backgroundRefreshEnabled

Gibt an, ob der Token-Anbieter das Token im Hintergrund aktualisieren soll. Wenn Sie dies festlegen, aktualisiert der Token-Anbieter im Hintergrund Ihre Token gemäß den Konfigurationseinstellungen, die die Aktivitäten zur automatischen Token-Aktualisierung regeln.

Erforderlich: Nein

Typ: Boolean

Standardwert: TRUE

domainName

Die im Token zu verwendende Domain, die bei der Token-Erfassung und Speicherung von Cookies verwendet wird. Zum Beispiel `example.com` oder `aws.amazon.com`. Dies

ist normalerweise die Hostdomäne Ihrer Ressource, die mit der Web-ACL verknüpft ist, an die Sie Webanfragen senden werden. Für die verwaltete ACFP-Regelgruppe ist dies normalerweise eine einzelne Domäne `AWSManagedRulesACFPRuleSet`, die der Domäne im Kontoerstellungspfad entspricht, den Sie in der Regelgruppenkonfiguration angegeben haben. Bei der von ATP verwalteten Regelgruppe `AWSManagedRulesATPRuleSet` handelt es sich in der Regel um eine einzelne Domäne, die der Domäne in dem Anmeldepfad entspricht, den Sie in der Regelgruppenkonfiguration angegeben haben.

Öffentliche Suffixe sind nicht zulässig. Beispielsweise können Sie `gov.au` oder nicht `co.uk` als Token-Domain verwenden.

Die Domain muss akzeptiert AWS WAF werden, basierend auf der geschützten Host-Domain und der Token-Domainliste der Web-ACL. Weitere Informationen finden Sie unter [Konfiguration der Domainliste für Web-ACL-Tokens](#).

Erforderlich: Ja

Typ: `String`

`maxErrorTokenRefreshDelayMsec`

Maximale Wartezeit in Millisekunden, bevor eine Token-Aktualisierung nach einem fehlgeschlagenen Versuch wiederholt wird. Dieser Wert wird verwendet, nachdem der Token-Abwurf fehlgeschlagen ist und `maxRetryCount`-mal erneut versucht wurde.

Erforderlich: Nein

Typ: `Integer`

Standardwert: `5000` (5 Sekunden)

Zulässiger Mindestwert: `1` (1 Millisekunde)

Zulässiger Höchstwert: `30000` (30 Sekunden)

`maxRetryCount`

Die maximale Anzahl von Wiederholungen, die mit exponentiellem Backoff ausgeführt werden sollen, wenn ein Token angefordert wird.

Erforderlich: Nein

Typ: `Integer`

Standardwert: Wenn die Hintergrundaktualisierung aktiviert ist, 5. Andernfalls 3.

Zulässiger Mindestwert: 0

Zulässiger Höchstwert: 10

setTokenCookie

Gibt an, ob der Cookie-Manager des SDK Ihren Anforderungen ein Token-Cookie hinzufügen soll. Standardmäßig wird allen Anforderungen ein Token-Cookie hinzugefügt. Der Cookie-Manager fügt jeder Anforderung ein Token-Cookie hinzu, deren Pfad unter dem in `tokenCookiePath` angegebenen liegt.

Erforderlich: Nein

Typ: Boolean

Standardwert: TRUE

tokenCookiePath

Wird verwendet wenn `setTokenCookie` TRUE ist. Gibt den obersten Pfad an, auf dem der Cookie-Manager des SDK ein Token-Cookie hinzufügen soll. Der Manager fügt allen Anforderungen, die Sie an diesen Pfad und an alle untergeordneten Pfade senden, ein Token-Cookie hinzu.

Wenn Sie hierfür beispielsweise `/web/login` festlegen, schließt der Manager das Token-Cookie für alles ein, was an `/web/login` und sämtliche untergeordneten Pfade, etwa `/web/login/help`, gesendet wird. Nicht enthalten ist das Token für Anforderungen, die an andere Pfade gesendet werden, etwa `/`, `/web` oder `/web/order`.

Erforderlich: Nein

Typ: String

Standardwert: /

tokenRefreshDelaySec

Wird für die Hintergrundaktualisierung verwendet. Die maximale Zeitspanne in Sekunden zwischen den Hintergrundaktualisierungen des Tokens wird angezeigt.

Erforderlich: Nein

Typ: Integer

Standardwert: 88

Zulässiger Mindestwert: 88

Zulässiger Höchstwert: 300 (5 Minuten)

So funktioniert das SDK AWS WAF für Mobilgeräte

Die SDKs für Mobilgeräte bieten Ihnen einen konfigurierbaren Token-Anbieter, den Sie für den Abruf und die Verwendung von Token verwenden können. Der Token-Anbieter überprüft, ob die von Ihnen zugelassenen Anforderungen von legitimen Kunden stammen. Wenn Sie Anfragen an die AWS Ressourcen senden, mit denen Sie sich schützen AWS WAF, fügen Sie das Token in ein Cookie ein, um die Anfrage zu validieren. Sie können das Token-Cookie manuell bearbeiten oder die Bearbeitung dem Token-Anbieter überlassen.

In diesem Abschnitt werden die Interaktionen zwischen den Klassen, Eigenschaften und Methoden behandelt, die im mobilen SDK enthalten sind. Informationen zur SDK-Spezifikation finden Sie unter [Die AWS WAF mobile SDK-Spezifikation](#).

Abrufen und Caching von Token

Wenn Sie die Instance des Token-Anbieters in Ihrer mobilen App erstellen, konfigurieren Sie, wie Sie Token und den Abruf von Token verwalten möchten. In erster Linie müssen Sie festlegen, wie gültige, nicht abgelaufene Token für die Verwendung in den Webanforderungen Ihrer App gepflegt werden sollen:

- Hintergrundaktualisierung aktiviert: Das ist die Standardeinstellung. Der Token-Anbieter aktualisiert das Token automatisch im Hintergrund und speichert es im Cache. Bei aktivierter Hintergrundaktualisierung wird das zwischengespeicherte Token abgerufen, wenn Sie `getToken()` aufrufen.

Der Token-Anbieter führt die Token-Aktualisierung in konfigurierbaren Intervallen durch, sodass ein nicht abgelaufenes Token immer im Cache verfügbar ist, während die Anwendung aktiv ist. Die Hintergrundaktualisierung wird angehalten, während sich Ihre Anwendung in einem inaktiven Zustand befindet. Weitere Informationen hierzu finden Sie unter [Abrufen eines Tokens nach App-Inaktivität](#).

- Hintergrundaktualisierung deaktiviert: Sie können die Hintergrundaktualisierung von Token deaktivieren und Token nur bei Bedarf abrufen. Bei Bedarf abgerufene Token werden nicht zwischengespeichert und Sie können mehrere abrufen, falls gewünscht. Jedes Token ist

unabhängig von anderen abgerufenen Token und verfügt jeweils über einen eigenen Zeitstempel, der zur Berechnung des Ablaufs verwendet wird.

Sie haben die folgenden Möglichkeiten für den Token-Abruf, wenn die Hintergrundaktualisierung deaktiviert ist:

- **getToken()**— Wenn Sie bei deaktivierter Aktualisierung im Hintergrund aufrufen `getToken()`, ruft der Aufruf synchron ein neues Token von ab. AWS WAF Dabei handelt es sich um einen potenziell blockierenden Aufruf, der sich im Hauptthread auf die Reaktionsfähigkeit der App auswirken kann.
- **onTokenReady(WAFTokenResultCallback)**: Bei diesem Aufruf wird asynchron ein neues Token abgerufen. Das bereitgestellte Ergebnis-Callback wird dann in einem Hintergrund-Thread aufgerufen, wenn ein Token bereit ist.

Wiederholen fehlgeschlagener Token-Abrufe durch den Token-Anbieter

Der Token-Anbieter wiederholt den Token-Abruf automatisch erneut, wenn er fehlgeschlagen ist. Wiederholungen werden zunächst mit exponentiellem Backoff mit einer Wartezeit von 100 ms durchgeführt. Hinweise zu exponentiellen Wiederholungen finden Sie unter [Fehlerwiederholungen](#) und exponentielles Backoff in. AWS

Wenn die Anzahl der Wiederholungen die konfigurierte `maxRetryCount` erreicht, stellt der Token-Anbieter die Versuche entweder ein oder versucht es ab sofort alle `maxErrorTokenRefreshDelayMsec` Millisekunden, abhängig von der Art des Token-Abrufs:

- **onTokenReady()**: Der Token-Anbieter wartet ab sofort `maxErrorTokenRefreshDelayMsec` Millisekunden zwischen den einzelnen Versuchen und versucht weiterhin, das Token abzurufen.
- Hintergrundaktualisierung: Der Token-Anbieter wartet ab sofort `maxErrorTokenRefreshDelayMsec` Millisekunden zwischen den einzelnen Versuchen und versucht weiterhin, das Token abzurufen.
- On-Demand-**getToken()**-Aufrufe, wenn die Hintergrundaktualisierung deaktiviert ist: Der Token-Anbieter versucht nicht mehr, ein Token abzurufen, und gibt den Wert des vorherigen Tokens oder einen Nullwert zurück, wenn kein vorheriges Token vorhanden ist.

Abrufen eines Tokens nach App-Inaktivität

Die Hintergrundaktualisierung wird nur durchgeführt, während Ihre App für Ihren App-Typ als aktiv gilt:

- iOS: Die Hintergrundaktualisierung wird durchgeführt, wenn sich die App im Vordergrund befindet.
- Android: Die Hintergrundaktualisierung wird durchgeführt, wenn die App nicht geschlossen wird, unabhängig davon, ob sie sich im Vordergrund oder im Hintergrund befindet.

Wenn Ihre App in einem Zustand verbleibt, der die Hintergrundaktualisierung länger als die konfigurierten `tokenRefreshDelaySec` Sekunden nicht unterstützt, unterbricht der Token-Anbieter die Hintergrundaktualisierung. Wenn beispielsweise für eine iOS-App die `tokenRefreshDelaySec` 300 beträgt und die App geschlossen wird oder länger als 300 Sekunden in den Hintergrund versetzt wird, aktualisiert der Token-Anbieter das Token nicht mehr. Wenn die App in einen aktiven Zustand zurückkehrt, startet der Token-Anbieter die Hintergrundaktualisierung automatisch neu.

Wenn Ihre App wieder in einen aktiven Zustand zurückkehrt, rufen Sie `onTokenReady()` auf, um benachrichtigt zu werden, wenn der Token-Anbieter ein neues Token abgerufen und zwischengespeichert hat. Rufen Sie nicht einfach `getToken()` auf, da der Cache möglicherweise noch kein aktuelles, gültiges Token enthält.

Schreiben Sie Ihren Code für das AWS WAF mobile SDK

Dieser Abschnitt enthält Beispiele für die Verwendung des SDK für Mobilgeräte.

Initialisieren des Token-Anbieters und Abrufen von Token

Sie initiieren die Instance des Token-Anbieters mit einem Konfigurationsobjekt. Dann können Sie Token mit den verfügbaren Operationen abrufen. Im Folgenden finden Sie die grundlegenden Benutzeroberflächenkomponenten des erforderlichen Codes.

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();
```

Zulassen, dass das SDK das Token-Cookie in Ihren HTTP-Anforderungen bereitstellt

Wenn `setTokenCookie` `TRUE` ist, stellt der Token-Anbieter das Token-Cookie in Ihren Webanforderungen an allen Standorten unter dem Pfad bereit, der in `tokenCookiePath` angegeben wurde. Standardmäßig ist `setTokenCookie` `TRUE` und `tokenCookiePath` ist `/`.

Sie schränken den Umfang der Anforderungen, die ein Token-Cookie enthalten, ein, indem Sie den Token-Cookie-Pfad angeben, zum Beispiel `/web/login`. Stellen Sie in diesem Fall sicher, dass Ihre AWS WAF Regeln in den Anfragen, die Sie an andere Pfade senden, nicht nach Tokens suchen. Wenn Sie die `AWSManagedRulesACFPRuleSet` Regelgruppe verwenden, konfigurieren Sie die Pfade zur Kontoregistrierung und Kontoerstellung, und die Regelgruppe sucht in Anfragen, die an diese Pfade gesendet werden, nach Tokens. Weitere Informationen finden Sie unter [Hinzufügen der verwalteten ACFP-Regelgruppe zu Ihrer Web-ACL](#). Wenn Sie die `AWSManagedRulesATPRuleSet` Regelgruppe verwenden, konfigurieren Sie auf ähnliche Weise den Anmeldepfad, und die Regelgruppe sucht in Anfragen, die an diesen Pfad gesendet werden, nach Tokens. Weitere Informationen finden Sie unter [Hinzufügen der von ATP verwalteten Regelgruppe zu Ihrer Web-ACL](#).

iOS

Wenn `setTokenCookie` `jaTRUE`, speichert der Token-Anbieter das AWS WAF Token in einer `HTTPCookieStorage.shared` und nimmt das Cookie automatisch in Anfragen an die Domain auf, in der Sie angegeben haben `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 `setTokenCookie` diesem `TRUE` Fall speichert der Token-Anbieter das AWS WAF Token in einer `CookieHandler` Instanz, die für die gesamte Anwendung gemeinsam genutzt wird. Der Token-Anbieter schließt das Cookie automatisch in Anforderungen an die Domäne ein, die Sie in der `WAFConfiguration` angegeben haben.

```
URL url = new URL("Domain name");
```

```
//The token cookie is set automatically as cookie header
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
connection.getResponseCode();
```

Wenn Sie die `CookieHandler`-Standard-Instanz bereits initialisiert haben, nutzt der Token-Anbieter diese zur Verwaltung von Cookies. Wenn nicht, initialisiert der Token-Anbieter eine neue `CookieManager` Instanz mit dem AWS WAF Token `CookiePolicy.ACCEPT_ORIGINAL_SERVER` und legt diese neue Instanz dann als Standardinstanz in `CookieHandler` fest.

Der folgende Code zeigt, wie das SDK den Cookie-Manager und den Cookie-Handler initialisiert, wenn diese in Ihrer App nicht verfügbar sind.

```
CookieManager cookieManager = (CookieManager) CookieHandler.getDefault();
if (cookieManager == null) {
    // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
    cookieManager = new CookieManager();
    CookieHandler.setDefault(cookieManager);
}
```

Manuelles Bereitstellen des Token-Cookies in Ihren HTTP-Anforderungen

Wenn Sie `setTokenCookie` auf `FALSE` festlegen, müssen Sie das Token-Cookie manuell als Cookie-HTTP-Anforderungsheader in den Anforderungen an Ihren geschützten Endpunkt bereitstellen. Der folgende Code veranschaulicht, wie dazu vorgegangen wird.

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();
```

CAPTCHA und Challenge in AWS WAF

Sie können Ihre AWS WAF Regeln so konfigurieren, dass eine CAPTCHA oder eine Challenge Aktion gegen Webanfragen ausgeführt wird, die den Prüfkriterien Ihrer Regel entsprechen. Sie können Ihre JavaScript Client-Anwendungen auch so programmieren, dass sie CAPTCHA-Rätsel und Browser-Herausforderungen lokal ausführen.

- **CAPTCHA**— Erfordert, dass der Endbenutzer ein CAPTCHA-Rätsel löst, um nachzuweisen, dass ein Mensch die Anfrage sendet. CAPTCHA-Rätsel sollen für Menschen relativ einfach und schnell erfolgreich zu lösen sein und für Computer schwierig sein, entweder erfolgreich oder nach dem Zufallsprinzip mit einer nennenswerten Erfolgsquote zu lösen.

In Web-ACL-Regeln wird CAPTCHA häufig verwendet, wenn durch eine Block Aktion zu viele legitime Anfragen gestoppt würden, aber der gesamte Datenverkehr durchgelassen würde, würde dies zu einer inakzeptabel hohen Anzahl unerwünschter Anfragen führen, z. B. von Bots. Informationen zum Verhalten der Regelaktion finden Sie unter [So funktionieren die Aktionen CAPTCHA und Challenge Regeln](#)

Sie können auch eine CAPTCHA-Puzzle-Implementierung in Ihren APIs für die Client-Anwendungsintegration programmieren. Wenn Sie dies tun, können Sie das Verhalten und die Platzierung des Puzzles in Ihrer Client-Anwendung anpassen. Weitere Informationen finden Sie unter [AWS WAF Integration von Client-Anwendungen](#).

- **Challenge**— Führt eine unbeaufsichtigte Aufforderung aus, bei der in der Clientsitzung überprüft werden muss, ob es sich um einen Browser und nicht um einen Bot handelt. Die Überprüfung läuft im Hintergrund, ohne dass der Endbenutzer involviert ist. Dies ist eine gute Option, um Kunden zu verifizieren, von denen Sie vermuten, dass sie ungültig sind, ohne die Endbenutzererfahrung mit einem CAPTCHA-Puzzle negativ zu beeinflussen. Informationen zum Verhalten von Regelaktionen finden Sie unter [So funktionieren die Aktionen CAPTCHA und Challenge Regeln](#)

Die Challenge Regelaktion ähnelt der Herausforderung, die von den Client-APIs zur Integration intelligenter Bedrohungen ausgeführt wird. Eine Beschreibung finden Sie unter [AWS WAF Integration von Client-Anwendungen](#).

Note

Ihnen werden zusätzliche Gebühren berechnet, wenn Sie die Challenge Regelaktion CAPTCHA oder in einer Ihrer Regeln oder als Überschreibung von Regelaktionen in einer Regelgruppe verwenden. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).

Eine Beschreibung aller Aktionsoptionen für Regeln finden Sie unter [Regelaktion](#).

Themen

- [AWS WAF CAPTCHA-Rätsel](#)
- [So funktionieren die Aktionen CAPTCHA und Challenge Regeln](#)
- [Bewährte Methoden für die Verwendung der Challenge Aktionen CAPTCHA und](#)

AWS WAF CAPTCHA-Rätsel

AWS WAF bietet standardmäßige CAPTCHA-Funktionen, bei denen Benutzer bestätigen müssen, dass sie Menschen sind. CAPTCHA steht für Completely Automated Public Turing Test to tell Computers and Human Apart. CAPTCHA-Rätsel dienen dazu, zu überprüfen, ob ein Mensch Anfragen sendet, und Aktivitäten wie Web-Scraping, Credential-Stuffing und Spam zu verhindern. CAPTCHA-Rätsel können nicht alle unerwünschten Anfragen aussortieren. Viele Rätsel wurden mithilfe von maschinellem Lernen und künstlicher Intelligenz gelöst. In dem Bemühen, CAPTCHA zu umgehen, ergänzen einige Organisationen automatisierte Techniken durch menschliches Eingreifen. Trotzdem ist CAPTCHA nach wie vor ein nützliches Instrument, um weniger ausgeklügelten Bot-Traffic zu verhindern und den Ressourcenbedarf für groß angelegte Operationen zu erhöhen.

AWS WAF generiert seine CAPTCHA-Rätsel nach dem Zufallsprinzip und durchläuft sie abwechselnd, um sicherzustellen, dass die Benutzer vor einzigartige Herausforderungen gestellt werden. AWS WAF fügt regelmäßig neue Arten und Stile von Rätseln hinzu, um gegen Automatisierungstechniken effektiv zu sein. Zusätzlich zu den Rätseln sammelt das AWS WAF CAPTCHA-Skript Daten über den Client, um sicherzustellen, dass die Aufgabe von einem Menschen erledigt wird, und um Wiederholungsangriffe zu verhindern.

Jedes CAPTCHA-Puzzle enthält eine Standardsteuerung, mit der der Endbenutzer ein neues Rätsel anfordern, zwischen Audio- und Videorätseln wechseln, auf zusätzliche Anweisungen zugreifen und eine Rätsellösung einreichen kann. Alle Rätsel bieten Unterstützung für Screenreader, Tastatursteuerung und kontrastierende Farben.

Die AWS WAF CAPTCHA-Rätsel erfüllen die Anforderungen der Web Content Accessibility Guidelines (WCAG). Weitere Informationen finden Sie unter [Web Content Accessibility Guidelines \(WCAG\) Overview](#) (Übersicht über die Zugänglichkeitsrichtlinien für Webinhalte (WCAG)) auf der Website des World Wide Web Consortium (W3C).

Themen

- [Unterstützung für CAPTCHA-Puzzlesprachen](#)
- [Beispiele für CAPTCHA-Rätsel](#)

Unterstützung für CAPTCHA-Puzzlesprachen

Das CAPTCHA-Puzzle beginnt mit schriftlichen Anweisungen in der Browsersprache des Clients oder, falls die Browsersprache nicht unterstützt wird, in Englisch. Das Rätsel bietet alternative Sprachoptionen über ein Drop-down-Menü.

Der Benutzer kann zu den Audioanweisungen wechseln, indem er das Kopfhörersymbol unten auf der Seite auswählt. Die Audioversion des Puzzles enthält gesprochene Anweisungen zu Text, den der Benutzer in ein Textfeld eingeben soll, wobei Hintergrundgeräusche überlagert werden.

In der folgenden Tabelle sind die Sprachen aufgeführt, die Sie für die schriftlichen Anweisungen in einem CAPTCHA-Puzzle auswählen können, sowie die Audiounterstützung für jede Auswahl.

AWS WAF Unterstützte Sprachen für das CAPTCHA-Puzzle

Unterstützung für schriftliche Anweisungen	Gebietsschema-Code	Unterstützung für Audioanweisungen
Arabisch	Ar-SA	Arabisch
Vereinfachtes Chinesisch	zh-CN	Audio auf Englisch
Niederländisch	nl-NL	Niederländisch
Englisch	en-US	Englisch
Französisch	fr-FR	Französisch

Unterstützung für schriftliche Anweisungen	Gebietsschema-Code	Unterstützung für Audioanweisungen
Deutsch	de-DE	Deutsch
Italienisch	it-IT	Italienisch
Japanisch	ja-JP	Audio auf Englisch
Brasilianisches Portugiesisch	pt-BR	Brasilianisches Portugiesisch
Spanisch	es-ES	Spanisch
Türkisch	tr-TR	Türkisch

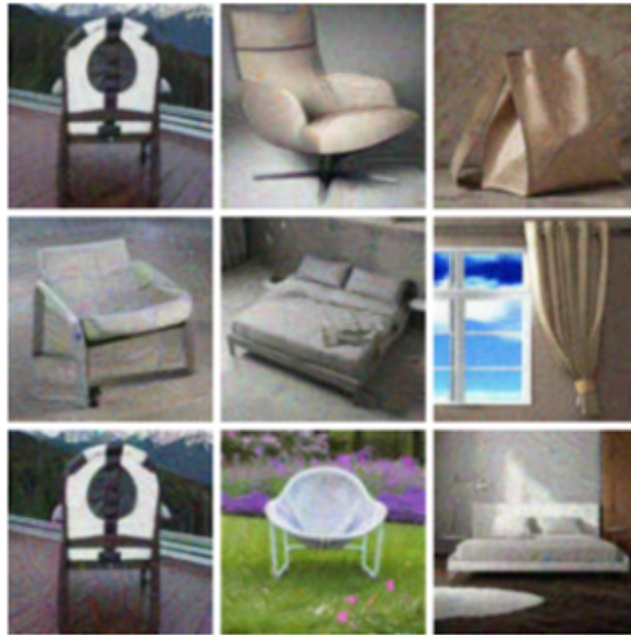
Beispiele für CAPTCHA-Rätsel

Ein typisches visuelles CAPTCHA-Puzzle erfordert Interaktion, um zu zeigen, dass der Benutzer ein oder mehrere Bilder verstehen und mit ihnen interagieren kann.

Der folgende Screenshot zeigt ein Beispiel für ein Bildraster-Puzzle. Bei diesem Rätsel müssen Sie alle Bilder im Raster auswählen, die einen bestimmten Objekttyp enthalten.

Let's confirm you are human

Choose all **the chairs**

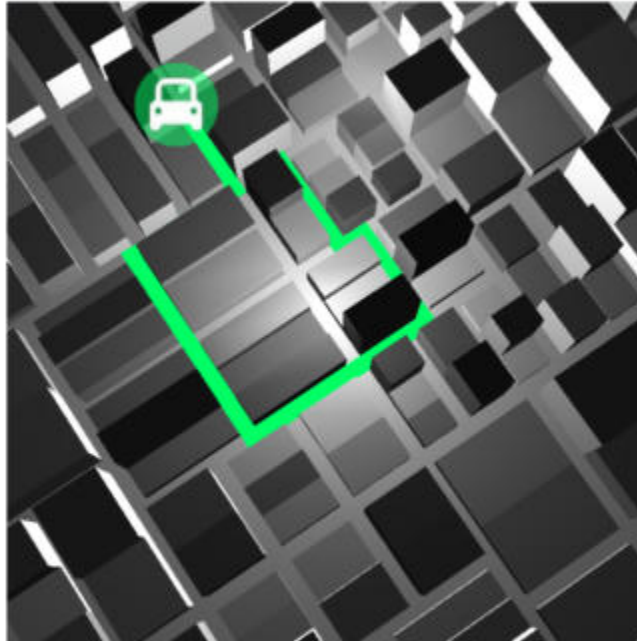


Confirm

Der folgende Screenshot zeigt ein Beispielrätsel, bei dem Sie den Endpunkt der Fahrbahn eines Autos in einer Zeichnung identifizieren müssen.

Solve the puzzle

Place a dot at the end of the car's path



English ▾

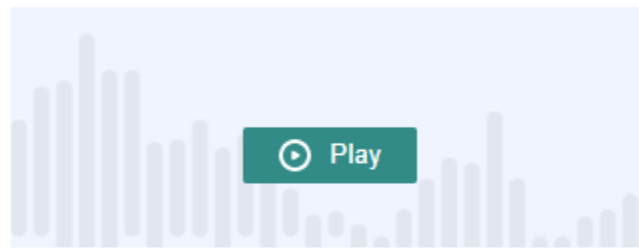
Submit

Ein Audiopuzzle bietet Hintergrundgeräusche, überlagert von gesprochenen Anweisungen zu Text, den der Benutzer in ein Textfeld eingeben sollte.

Im folgenden Screenshot sehen Sie das Display für die Audio-Rätsel-Auswahl.

Solve the puzzle



Click play to listen to instructions






Keyboard audio toggle: alt + space

Enter your response

Answer

Solve by listening to the recording and typing your answer into the text box.  

Submit

So funktionieren die Aktionen CAPTCHA und Challenge Regeln

AWS WAF CAPTCHA und Challenge sind Standardregelaktionen, sodass sie relativ einfach zu implementieren sind. Um eine von beiden zu verwenden, erstellen Sie die Prüfkriterien für Ihre Regel, die die Anfragen identifiziert, die Sie überprüfen möchten, und geben dann eine der beiden Regelaktionen an. Allgemeine Informationen zu den Optionen für die Regelaktionen finden Sie unter [Regelaktion](#).

Sie können nicht nur stille Herausforderungen und CAPTCHA-Rätsel serverseitig implementieren, sondern auch stille Herausforderungen in Ihre iOS JavaScript - und Android-Client-Anwendungen integrieren und CAPTCHA-Rätsel in Ihren Clients rendern. JavaScript Diese Integrationen ermöglichen es Ihnen, Ihren Endbenutzern eine bessere Leistung und bessere CAPTCHA-Rätselerlebnisse zu bieten. Außerdem können sie die Kosten senken, die mit der Verwendung der Regelaktionen und der intelligenten Regelgruppen zur Bedrohungsabwehr verbunden sind. Weitere Informationen zu diesen Optionen finden Sie unter [AWS WAF Integration von Client-Anwendungen](#). Preisinformationen finden Sie unter [AWS WAF – Preise](#).

Themen

- [CAPTCHA und Challenge Handlungsverhalten](#)
- [CAPTCHA und Challenge Aktionen in den Protokollen und Metriken](#)

CAPTCHA und Challenge Handlungsverhalten

Wenn eine Webanforderung den Prüfkriterien einer Regel mit CAPTCHA oder einer Challenge Aktion entspricht, AWS WAF wird anhand des Status des Tokens und der Konfiguration der Immunitätszeit festgelegt, wie die Anfrage behandelt werden soll. AWS WAF berücksichtigt auch, ob die Anfrage die CAPTCHA-Puzzle- oder Challenge-Skriptinterstitials verarbeiten kann. Die Skripts sind so konzipiert, dass sie als HTML-Inhalt behandelt werden können, und sie können nur von einem Client korrekt verarbeitet werden, der HTML-Inhalt erwartet.

Note

Ihnen werden zusätzliche Gebühren berechnet, wenn Sie die Challenge Regelaktion CAPTCHA oder in einer Ihrer Regeln oder als Überschreibung von Regelaktionen in einer Regelgruppe verwenden. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).


Wie die Aktion mit der Webanfrage umgeht

AWS WAF wendet die Challenge Aktion CAPTCHA oder wie folgt auf eine Webanforderung an:

- Gültiges Token — AWS WAF behandelt dies ähnlich wie eine Count Aktion. AWS WAF wendet alle Labels an und fordert Anpassungen an, die Sie für die Regelaktion konfiguriert haben, und bewertet dann die Anforderung anhand der verbleibenden Regeln in der Web-ACL weiter.
- Fehlendes, ungültiges oder abgelaufenes Token — beendet AWS WAF die Web-ACL-Auswertung der Anfrage und verhindert, dass sie an ihr beabsichtigtes Ziel weitergeleitet wird.


AWS WAF generiert eine Antwort, die entsprechend dem Aktionstyp der Regel an den Client zurückgesendet wird:

- Challenge— AWS WAF schließt Folgendes in die Antwort ein:
 - Den Header `x-amzn-waf-action` mit einem Wert von `challenge`.

 Note

Dieser Header ist für JavaScript Anwendungen, die im Client-Browser ausgeführt werden, nicht verfügbar. Einzelheiten finden Sie im folgenden Abschnitt.

- Den HTTP-Statuscode 202 Request Accepted.
- Wenn die Anfrage einen Accept Header mit dem Wert von enthält `text/html`, enthält die Antwort ein JavaScript Seiteninterstitial mit einem Challenge-Skript.
- CAPTCHA— AWS WAF beinhaltet Folgendes in der Antwort:
 - Den Header `x-amzn-waf-action` mit einem Wert von `captcha`.

 Note

Dieser Header ist für JavaScript Anwendungen, die im Client-Browser ausgeführt werden, nicht verfügbar. Einzelheiten finden Sie im folgenden Abschnitt.

- Den HTTP-Statuscode 405 Method Not Allowed.
- Wenn die Anfrage einen Accept Header mit dem Wert von enthält `text/html`, enthält die Antwort ein JavaScript Seiteninterstitial mit einem CAPTCHA-Skript.

Informationen zur Konfiguration des Ablaufs von Token auf Web-ACL- oder Regelebene finden Sie unter [Ablauf des Zeitstempels: Zeiten der Token-Immunität](#)

Header sind für JavaScript Anwendungen, die im Clientbrowser ausgeführt werden, nicht verfügbar

Wenn AWS WAF auf eine Client-Anfrage mit einem CAPTCHA oder einer Challenge-Antwort geantwortet wird, sind keine CORS-Header (Cross-Origin Resource Sharing) enthalten. CORS-Header sind eine Reihe von Zugriffskontroll-Headern, die dem Client-Webbrowser mitteilen, welche Domänen, HTTP-Methoden und HTTP-Header von Anwendungen verwendet werden können. JavaScript Ohne CORS-Header erhalten JavaScript Anwendungen, die in einem Clientbrowser ausgeführt werden, keinen Zugriff auf HTTP-Header und können daher den in den Antworten und angegebenen `x-amzn-waf-action` Header nicht lesen. CAPTCHA Challenge

Was bewirken die Challenge und die CAPTCHA-Interstitials

Wenn ein Challenge-Interstitial ausgeführt wird, nachdem der Client erfolgreich geantwortet hat und er noch kein Token hat, initialisiert das Interstitial eines dafür. Dann aktualisiert es das Token mit dem Zeitstempel für die Problemlösung.

Wenn ein CAPTCHA-Interstitial ausgeführt wird und der Client noch kein Token hat, ruft das CAPTCHA-Interstitial zuerst das Challenge-Skript auf, um den Browser herauszufordern und das Token zu initialisieren. Dann führt das Interstitial sein CAPTCHA-Puzzle aus. Wenn der Endbenutzer das Rätsel erfolgreich gelöst hat, aktualisiert das Interstitial das Token mit dem CAPTCHA-Lösungszeitstempel.

In beiden Fällen sendet das Skript, nachdem der Client erfolgreich geantwortet hat und das Skript das Token aktualisiert hat, die ursprüngliche Webanfrage erneut mit dem aktualisierten Token.

Sie können konfigurieren, wie mit Tokens AWS WAF umgegangen wird. Weitere Informationen finden Sie unter [AWS WAF Webanforderungstoken](#).

CAPTCHA und Challenge Aktionen in den Protokollen und Metriken

Die Challenge Aktionen CAPTCHA und können nicht beendend, ähnlich, oder Count beendend, ähnlich sein. Block Das Ergebnis hängt davon ab, ob die Anfrage ein gültiges Token mit einem nicht abgelaufenen Zeitstempel für den Aktionstyp enthält.

- Gültiges Token — Wenn die Aktion ein gültiges Token findet und die Anfrage nicht blockiert, werden Metriken und Protokolle wie folgt AWS WAF erfasst:
 - Inkrementiert die Metriken für entweder `CaptchaRequests` und `RequestsWithValidCaptchaToken` oder `ChallengeRequests` und `RequestsWithValidChallengeToken`.
 - Protokolliert den Treffer als `nonTerminatingMatchingRules` Eintrag mit der Aktion CAPTCHA oder Challenge. Die folgende Liste zeigt den Abschnitt eines Protokolls für diesen Übereinstimmungstyp mit der CAPTCHA Aktion.

```
"nonTerminatingMatchingRules": [  
  {  
    "ruleId": "captcha-rule",  
    "action": "CAPTCHA",  
    "ruleMatchDetails": [],  
    "captchaResponse": {  
      "responseCode": 0,  
      "solveTimestamp": 1632420429  
    }  
  }  
]
```



```

    }
  ]

```

- Fehlendes, ungültiges oder abgelaufenes Token — Wenn die Aktion die Anfrage aufgrund eines fehlenden oder ungültigen Tokens blockiert, werden Metriken und Protokolle wie folgt AWS WAF erfasst:
 - Inkrementiert die Metrik für `CaptchaRequests` oder `ChallengeRequests`.
 - Protokolliert den Treffer als `CaptchaResponse` Eintrag mit 405 HTTP-Statuscode oder als `ChallengeResponse` Eintrag mit 202 HTTP-Statuscode. Das Protokoll gibt an, ob bei der Anfrage das Token fehlte oder ob der Zeitstempel abgelaufen war. Aus dem Protokoll geht auch hervor, ob eine CAPTCHA-Zwischenseite an den Client oder eine unbeaufsichtigte Aufforderung an den Client-Browser AWS WAF gesendet wurde. Die folgende Liste zeigt die Abschnitte eines Protokolls für diesen Typ von Übereinstimmung mit der Aktion. CAPTCHA

```

"terminatingRuleId": "captcha-rule",
"terminatingRuleType": "REGULAR",
"action": "CAPTCHA",
"terminatingRuleMatchDetails": [],
...
"responseCodeSent": 405,
...
"captchaResponse": {
  "responseCode": 405,
  "solveTimestamp": 0,
  "failureReason": "TOKEN_MISSING"
}

```

Informationen zu den AWS WAF Protokollen finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).

Informationen zu AWS WAF Metriken finden Sie unter [AWS WAF Metriken und Dimensionen](#).

Informationen zu den Optionen für die Regelaktionen finden Sie unter [Regelaktion](#).

Bewährte Methoden für die Verwendung der Challenge Aktionen CAPTCHA und

Folgen Sie den Anweisungen in diesem Abschnitt, um AWS WAF CAPTCHA oder Challenge zu planen und zu implementieren.

Plane dein CAPTCHA und fordere die Implementierung heraus

Entscheiden Sie anhand der Nutzung Ihrer Website, der Vertraulichkeit der zu schützenden Daten und der Art der Anfragen, wo Sie CAPTCHA-Rätsel oder stille Herausforderungen platzieren möchten. Wählen Sie die Anfragen aus, bei denen Sie CAPTCHA anwenden möchten, sodass Sie die Rätsel nach Bedarf präsentieren. Vermeiden Sie es jedoch, sie dort zu präsentieren, wo sie nicht nützlich wären und die Benutzererfahrung beeinträchtigen könnten. Verwenden Sie die Challenge Aktion, um Anfragen im Hintergrund auszuführen, die weniger Auswirkungen auf den Endbenutzer haben, aber dennoch sicherstellen, dass die Anfrage von einem JavaScript aktivierten Browser stammt.

Entscheiden Sie, wo Sie CAPTCHA-Rätsel und stille Herausforderungen für Ihre Kunden ausführen möchten

Identifizieren Sie Anfragen, die Sie nicht durch CAPTCHA beeinflussen lassen möchten, z. B. Anfragen nach CSS oder Bildern. Verwenden Sie CAPTCHA nur bei Bedarf. Wenn Sie beispielsweise eine CAPTCHA-Prüfung bei der Anmeldung planen und der Benutzer immer direkt von der Anmeldung zu einem anderen Bildschirm weitergeleitet wird, wäre eine CAPTCHA-Prüfung auf dem zweiten Bildschirm wahrscheinlich nicht erforderlich, was Ihre Benutzererfahrung beeinträchtigen könnte.

Konfigurieren Sie Challenge und CAPTCHA so, dass AWS WAF nur CAPTCHA-Rätsel und stille Herausforderungen als Antwort auf Anfragen gesendet werden. GET text/html Sie können weder das Rätsel noch die Herausforderung als Antwort auf POST Anfragen, CORS-Preflight-Anfragen (Cross-Origin Resource Sharing) oder andere Typen ausführen, die keine OPTIONS Anfragen sind. GET Das Browserverhalten für andere Anforderungstypen kann variieren und kann die Interstitials möglicherweise nicht richtig verarbeiten.

Es ist möglich, dass ein Client HTML akzeptiert, aber trotzdem nicht in der Lage ist, mit dem CAPTCHA oder dem Challenge-Interstitial umzugehen. Beispielsweise akzeptiert ein Widget auf einer Webseite mit einem kleinen iFrame möglicherweise HTML, ist aber nicht in der Lage, ein CAPTCHA anzuzeigen oder zu verarbeiten. Vermeiden Sie es, die Regelaktionen für diese Art von Anfragen zu platzieren, genauso wie für Anfragen, die kein HTML akzeptieren.

Verwenden Sie CAPTCHA oder Challenge, um den vorherigen Token-Erwerb zu überprüfen

Sie können die Regelaktionen ausschließlich dazu verwenden, das Vorhandensein eines gültigen Tokens zu überprüfen, und zwar an Orten, an denen legitime Benutzer immer über eines verfügen sollten. In diesen Situationen spielt es keine Rolle, ob die Anfrage die Interstitials verarbeiten kann.

Wenn Sie beispielsweise die CAPTCHA-API der JavaScript Client-Anwendung implementieren und das CAPTCHA-Puzzle unmittelbar vor dem Senden der ersten Anfrage an Ihren geschützten

Endpunkt auf dem Client ausführen, sollte Ihre erste Anfrage immer ein Token enthalten, das sowohl für Challenge als auch für CAPTCHA gültig ist. Informationen JavaScript zur Integration von Client-Anwendungen finden Sie unter [AWS WAF JavaScript Integrationen](#)

In diesem Fall können Sie in Ihrer Web-ACL eine Regel hinzufügen, die mit diesem ersten Aufruf übereinstimmt, und sie mit der CAPTCHA Regelaktion Challenge oder konfigurieren. Wenn die Regel für einen legitimen Endbenutzer und einen legitimen Browser zutrifft, findet die Aktion ein gültiges Token, sodass die Anfrage nicht blockiert wird und keine Aufforderung oder ein CAPTCHA-Rätsel als Antwort gesendet wird. Weitere Informationen zur Funktionsweise der Regelaktionen finden Sie unter [CAPTCHA und Challenge Handlungsverhalten](#)

Schützen Sie Ihre sensiblen Nicht-HTML-Daten mit und CAPTCHA Challenge

Sie können CAPTCHA und Challenge Schutzmaßnahmen für sensible Nicht-HTML-Daten wie APIs mit dem folgenden Ansatz verwenden.

1. Identifizieren Sie Anforderungen, die HTML-Antworten akzeptieren und die in unmittelbarer Nähe der Anforderungen für Ihre sensiblen, nicht HTML-Daten ausgeführt werden.
2. Schreiben Sie CAPTCHA oder Challenge Regeln, die mit den HTML-Anfragen und den Anfragen nach Ihren vertraulichen Daten übereinstimmen.
3. Passen Sie Ihre Einstellungen CAPTCHA und die Challenge Immunitätszeit so an, dass bei normalen Benutzerinteraktionen die Token, die Kunden aus den HTML-Anfragen erhalten, in ihren Anfragen nach Ihren sensiblen Daten verfügbar sind und nicht abgelaufen sind. Informationen zur Optimierung finden Sie unter [Ablauf des Zeitstempels: Zeiten der Token-Immunität](#).

Wenn eine Anfrage für Ihre sensiblen Daten einer CAPTCHA Challenge OR-Regel entspricht, wird sie nicht blockiert, sofern der Kunde noch über ein gültiges Token aus dem vorherigen Rätsel oder der vorherigen Herausforderung verfügt. Wenn das Token nicht verfügbar ist oder der Zeitstempel abgelaufen ist, schlägt die Anfrage zum Zugriff auf Ihre sensiblen Daten fehl. Weitere Informationen zur Funktionsweise der Regelaktionen finden Sie unter [CAPTCHA und Challenge Handlungsverhalten](#).

Verwenden Sie CAPTCHA und passen Sie Ihre bestehenden Regeln Challenge an

Überprüfen Sie Ihre bestehenden Regeln, um zu sehen, ob Sie sie ändern oder ergänzen möchten. Im Folgenden werden einige gängige Szenarien vorgestellt.

- Wenn Sie eine ratenbasierte Regel haben, die den Datenverkehr blockiert, Sie das Ratenlimit jedoch relativ hoch halten, um zu verhindern, dass legitime Benutzer blockiert werden, sollten Sie erwägen, nach der Sperrregel eine zweite ratenbasierte Regel hinzuzufügen. Geben Sie der

zweiten Regel ein niedrigeres Limit als der Sperrregel und legen Sie die Regelaktion auf oder fest. CAPTCHA Challenge Die Blockierungsregel blockiert weiterhin Anfragen, die mit einer zu hohen Rate eingehen, und die neue Regel blockiert den größten Teil des automatisierten Datenverkehrs mit einer noch niedrigeren Rate. Weitere Informationen über ratenbasierte Regeln finden Sie unter [Ratenbasierte Regelanweisung](#).

- Wenn Sie über eine verwaltete Regelgruppe verfügen, die Anfragen blockiert, können Sie das Verhalten einiger oder aller Regeln von Block auf CAPTCHA oder ändern Challenge. Überschreiben Sie dazu in der Konfiguration der verwalteten Regelgruppe die Einstellung für die Regelaktion. Informationen zum Außerkraftsetzen von Regelaktionen finden Sie unter [Regelaktionen überschreiben](#).

Testen Sie Ihre CAPTCHA- und Challenge-Implementierungen, bevor Sie sie bereitstellen

Bezüglich aller neuen Funktionen folgen Sie den Anweisungen unter [the section called “Testen und Optimieren Ihrer Schutzmaßnahmen”](#)

Überprüfen Sie während des Tests die Ablaufanforderungen für den Token-Zeitstempel und richten Sie Ihre Web-ACL- und Immunitätszeitkonfigurationen auf Regelebene so ein, dass Sie ein ausgewogenes Verhältnis zwischen der Kontrolle des Zugriffs auf Ihre Website und der Bereitstellung eines guten Benutzererlebnisses für Ihre Kunden erreichen. Weitere Informationen finden Sie unter [Ablauf des Zeitstempels: Zeiten der Token-Immunität](#).

AWS WAF Web-ACL-Verkehr protokollieren

Sie können die Protokollierung aktivieren, um detaillierte Informationen über den Traffic zu erhalten, der von Ihrer Web-ACL analysiert wird. Zu den protokollierten Informationen gehören die Uhrzeit, zu der eine Webanfrage von Ihrer AWS Ressource AWS WAF eingegangen ist, detaillierte Informationen zu der Anfrage und Details zu den Regeln, denen die Anfrage entsprach. Sie können Ihre Protokolle an eine Amazon CloudWatch Logs-Protokollgruppe, einen Amazon Simple Storage Service (Amazon S3) -Bucket oder eine Amazon Data Firehose senden.

Note

Die Protokollierungskonfiguration wirkt sich nur auf die AWS WAF Protokolle aus. Insbesondere die Konfiguration der geschwärzten Felder für die Protokollierung hat keinen Einfluss auf das Sampling von Anfragen. Die einzige Möglichkeit, Felder aus gesampelten Anfragen auszuschließen, besteht darin, das Sampling für die Web-ACL zu deaktivieren.

Wenn Sie in Ihren Protokollen keinen Protokolleintrag finden können

In seltenen Fällen ist es möglich, dass die AWS WAF Protokollzustellung unter 100% fällt, wobei die Protokolle nach bestem Wissen und Gewissen geliefert werden. Die AWS WAF Architektur räumt der Sicherheit Ihrer Anwendungen Vorrang vor allen anderen Überlegungen ein. In einigen Situationen, z. B. wenn bei Protokollierungsabläufen der Datenverkehr eingeschränkt wird, kann dies dazu führen, dass Datensätze gelöscht werden. Dies sollte sich nicht auf mehr als ein paar Datensätze auswirken. Wenn Sie feststellen, dass eine Reihe von Protokolleinträgen fehlt, wenden Sie sich an das [AWS Support Center](#).

Themen

- [Preise für die Protokollierung von Web-ACL-Datenverkehrsinformationen](#)
- [AWS WAF Ziele protokollieren](#)
- [Verwalten der Protokollierung für eine Web-ACL](#)
- [Protokollfelder](#)
- [Beispiele protokollieren](#)

Preise für die Protokollierung von Web-ACL-Datenverkehrsinformationen

Die Kosten für die Protokollierung des Web-ACL-Datenverkehrs richten sich nach den Kosten, die mit den einzelnen Protokollzieltypen verbunden sind. Diese Gebühren gelten zusätzlich zu den Gebühren für die Verwendung von AWS WAF. Die Kosten hängen von Faktoren wie dem gewählten Zielort und der Menge der aufgezeichneten Daten ab.

Nachfolgend finden Sie Links zu den Preisinformationen für die einzelnen Zieltypen der Protokollierung:

- CloudWatch Protokolle — Die Gebühren beziehen sich auf die Lieferung von Protokollen im Verkauf. Weitere Informationen finden Sie unter [Amazon CloudWatch Logs-Preise](#). Wählen Sie unter Bezahltes Kontingent den Tab Logs und dann unter Vended Logs die Informationen für Delivery to CloudWatch Logs.
- Amazon S3-Buckets — Die Amazon S3 S3-Gebühren sind die kombinierten Gebühren für die Lieferung von CloudWatch Logs an die Amazon S3 S3-Buckets und für die Nutzung von Amazon S3.
 - Weitere Informationen zu Amazon S3 finden Sie unter [Amazon S3 Pricing](#) (Preise für Amazon S3).

- Informationen zur Lieferung von CloudWatch Logs an Amazon S3 finden Sie unter [Amazon CloudWatch Logs-Preise](#). Wählen Sie unter Paid Tier (Kostenpflichtiges Kontingent) die Registerkarte Logs (Protokolle). Unter Vended Logs (Vended-Protokolle) finden Sie die Informationen zu Delivery to S3 (Lieferung an S3).
- Firehose — Sehen Sie sich die [Amazon Data Firehose-Preise](#) an.

[Informationen zur AWS WAF Preisgestaltung finden Sie unter AWS WAF Preise.](#)

AWS WAF Ziele protokollieren

In diesem Abschnitt werden die Protokollierungsoptionen beschrieben, aus denen Sie für Ihre AWS WAF Protokolle wählen können. Jeder Abschnitt enthält Anleitungen zur Konfiguration der Protokollierung, einschließlich Informationen zu jeglichem Verhalten, das für den Zieltyp spezifisch ist. Nachdem Sie das Logging-Ziel konfiguriert haben, können Sie dessen Spezifikationen für Ihre Web-ACL-Logging-Konfiguration angeben, um mit der Protokollierung zu beginnen.

Themen

- [CloudWatch Amazon-Protokolle](#)
- [Amazon Simple Storage Service](#)
- [Amazon Data Firehose](#)

CloudWatch Amazon-Protokolle

Dieses Thema enthält Informationen zum Senden Ihrer Web-ACL-Traffic-Logs an eine CloudWatch Logs-Protokollgruppe.

Note

Die Kosten für die Protokollierung werden zusätzlich zu den Kosten für die Nutzung von AWS WAF berechnet. Weitere Informationen finden Sie unter [Preise für die Protokollierung von Web-ACL-Datenverkehrsinformationen](#).

Um Protokolle an Amazon CloudWatch Logs zu senden, erstellen Sie eine CloudWatch Logs-Protokollgruppe. Wenn Sie die Anmeldung aktivieren AWS WAF, geben Sie den ARN der Protokollgruppe an. Nachdem Sie die Protokollierung für Ihre Web-ACL aktiviert haben, AWS WAF werden die CloudWatch Protokolle in Protokolldatenströmen an die Protokollgruppe Logs übermittelt.

Wenn Sie CloudWatch Logs verwenden, können Sie sich die Logs für Ihre Web-ACL in der AWS WAF Konsole ansehen. Wählen Sie auf Ihrer Web-ACL-Seite die Registerkarte Logging insights (Protokollierungseinblicke) aus. Diese Option ist eine Ergänzung zu den Protokollierungsergebnissen, die für CloudWatch Logs über die CloudWatch Konsole bereitgestellt werden.

Konfigurieren Sie die Protokollgruppe für AWS WAF Web-ACL-Protokolle in derselben Region wie die Web-ACL und verwenden Sie dasselbe Konto, das Sie für die Verwaltung der Web-ACL verwenden. Informationen zur Konfiguration einer CloudWatch Logs-Log-Gruppe finden Sie unter [Arbeiten mit Log-Gruppen und Log-Streams](#).

Kontingente für CloudWatch Log-Log-Gruppen

CloudWatch Logs hat standardmäßig ein maximales Kontingent für den Durchsatz, das auf alle Protokollgruppen innerhalb einer Region aufgeteilt wird und dessen Erhöhung Sie beantragen können. Wenn Ihre Protokollierungsanforderungen für die aktuelle Durchsatzeinstellung zu hoch sind, werden Ihnen Drosselungskennzahlen PutLogEvents für Ihr Konto angezeigt. Informationen zum Limit in der Konsole für Service Quotas und zur Beantragung einer Erhöhung finden Sie unter [CloudWatch PutLogEvents Protokollkontingent](#).

Benennung von Protokollgruppen

Die Namen Ihrer Protokollgruppen müssen mit `aws-waf-logs-` beginnen und können mit einem beliebigen Suffix enden, z. B. `aws-waf-logs-testLogGroup2`.

Das resultierende ARN-Format lautet folgendermaßen:

```
arn:aws:logs:Region:account-id:log-group:aws-waf-logs-log-group-suffix
```

Die Protokollstreams haben das folgende Benennungsformat:

```
Region_web-acl-name_log-stream-number
```

Im Folgenden wird ein Beispiel für einen Protokollstream für die Web-ACL TestWebACL in der Region `us-east-1` gezeigt.

```
us-east-1_TestWebACL_0
```

Zum Veröffentlichen von Protokollen in Logs sind Berechtigungen erforderlich CloudWatch

Für die Konfiguration der CloudWatch Web-ACL-Datenverkehrsprotokollierung für eine Logs-Protokollgruppe sind die in diesem Abschnitt beschriebenen Berechtigungseinstellungen erforderlich.

Die Berechtigungen werden für Sie festgelegt, wenn Sie eine der verwalteten Richtlinien AWS WAF mit vollem Zugriff verwenden, `AWSWAFConsoleFullAccess` oder `AWSWAFFullAccess`. Wenn Sie den Zugriff auf Ihre Protokollierung und AWS WAF Ressourcen detaillierter verwalten möchten, können Sie die Berechtigungen selbst festlegen. Informationen zur Verwaltung von Berechtigungen finden Sie unter [Zugriffsverwaltung für AWS Ressourcen](#) im IAM-Benutzerhandbuch. Weitere Informationen zu durch AWS WAF verwalteten Richtlinien finden Sie unter [AWS verwaltete Richtlinien für AWS WAF](#).

Mit diesen Berechtigungen können Sie die Web-ACL-Protokollierungskonfiguration ändern, die Protokollzustellung für CloudWatch Logs konfigurieren und Informationen über Ihre Log-Gruppe abrufen. Diese Berechtigungen müssen an den Benutzer angehängt werden, den Sie zur Verwaltung von AWS WAF verwenden.

```
{
  "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"
}
```



```
]
}
```

Wenn Aktionen für alle AWS Ressourcen zulässig sind, wird dies in der Richtlinie mit der "Resource" Einstellung von angegeben "*" ". Das bedeutet, dass die Aktionen für alle AWS Ressourcen zulässig sind, die jede Aktion unterstützt. Die Aktion `wafv2:PutLoggingConfiguration` wird beispielsweise nur für `wafv2`-Protokollkonfigurationsressourcen unterstützt.

Amazon Simple Storage Service

In diesem Thema finden Sie Informationen zum Senden Ihrer Web-ACL-Datenverkehrsprotokolle an einen Amazon-S3-Bucket.

Note

Die Kosten für die Protokollierung werden zusätzlich zu den Kosten für die Nutzung von AWS WAF berechnet. Weitere Informationen finden Sie unter [Preise für die Protokollierung von Web-ACL-Datenverkehrsinformationen](#).

Um Ihre Web-ACL-Traffic-Logs an Amazon S3 zu senden, richten Sie einen Amazon S3 S3-Bucket von demselben Konto aus ein, das Sie für die Verwaltung der Web-ACL verwenden, und geben dem Bucket einen Namen, der mit `beginntaws-waf-logs-`. Wenn Sie die Anmeldung aktivieren AWS WAF, geben Sie den Bucket-Namen an. Informationen zum Erstellen eines Logging-Buckets finden Sie unter [Create a Bucket](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Mit dem interaktiven Abfrageservice von Amazon Athena können Sie auf Ihre Amazon S3-Protokolle zugreifen und diese analysieren. Athena macht es einfach, Daten mit Standard-SQL direkt in Amazon S3 zu analysieren. Mit einigen Aktionen in der AWS Management Console können Sie Athena auf Ihre in Amazon S3 gespeicherten Daten verweisen und schnell beginnen, Standard-SQL zu verwenden, um Ad-hoc-Abfragen auszuführen und Ergebnisse zu erhalten. Weitere Informationen finden Sie unter [Abfragen von AWS WAF Protokollen](#) im Amazon Athena Athena-Benutzerhandbuch.

Note

AWS WAF unterstützt die Verschlüsselung mit Amazon S3 S3-Buckets für den Schlüsseltyp Amazon S3 S3-Schlüssel (SSE-S3) und für AWS Key Management Service (SSE-KMS).

AWS KMS keys AWS WAF unterstützt keine Verschlüsselung für AWS Key Management Service Schlüssel, die von verwaltet werden. AWS

Ihre Web-ACLs senden ihre Protokolldateien in 5-Minuten-Intervallen an den Amazon-S3-Bucket. Jede Protokolldatei enthält Aufzeichnungen über den Datenverkehr der letzten 5 Minuten.

Die maximale Dateigröße für eine Protokolldatei beträgt 75 MB. Wenn die Protokolldatei die Dateigrößenbeschränkung innerhalb des 5-Minuten-Zeitraums erreicht, fügt das Protokoll keine weiteren Protokollsätze hinzu, sondern veröffentlicht sie im Amazon-S3-Bucket und erstellt dann eine neue Protokolldatei.

Die Protokolldateien werden komprimiert. Wenn Sie die Dateien über die Amazon-S3-Konsole öffnen, dekomprimiert Amazon S3 die Protokollsätze und zeigt sie an. Wenn Sie die Protokolldateien herunterladen, müssen Sie sie dekomprimieren, um die Datensätze anzuzeigen.

Eine einzelne Protokolldatei enthält verschachtelte Einträge mit mehreren Datensätzen. Suchen Sie nach Einträgen, die nach dem Namen der Web-ACL, der Region und Ihrer Konto-ID zusammengefasst sind, um alle Protokolldateien für eine Web-ACL anzuzeigen.

Benennungsanforderungen und Syntax

Ihre Bucket-Namen für die AWS WAF Protokollierung müssen mit einem beliebigen Suffix beginnen `aws-waf-logs-` und können mit einem beliebigen Suffix enden. z. B. `aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX`.

Standort des Buckets

Die Speicherorte der Buckets verwenden die folgende Syntax:

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/
```

Bucket-ARN

Das Format des Buckets „Amazon-Ressourcenname (ARN)“ lautet wie folgt:

```
arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX
```

Bucket-Standorte mit Präfixen

Wenn Sie Präfixe in Ihrem Objektschlüsselnamen verwenden, um die Daten zu organisieren, die Sie in Ihren Buckets speichern, können Sie Ihre Präfixe in Ihren Logging-Bucket-Namen angeben.

Note

Diese Option ist nicht über die Konsole verfügbar. Verwenden Sie die AWS WAF APIs, CLI oder AWS CloudFormation.

Informationen zur Verwendung von Präfixen in Amazon S3 finden Sie unter [Objekte mithilfe von Präfixen organisieren](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Die Bucket-Standorte mit Präfixen verwenden die folgende Syntax:

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/DOC-EXAMPLE-KEY-NAME-PREFIX/
```

Bucket-Ordner und Dateinamen

In Ihren Buckets und nach allen von Ihnen angegebenen Präfixen werden Ihre AWS WAF Logs in eine Ordnerstruktur geschrieben, die durch Ihre Konto-ID, die Region, den Web-ACL-Namen sowie Datum und Uhrzeit bestimmt wird.

```
AWSLogs/account-id/WAFLogs/Region/web-acl-name/YYYY/MM/dd/HH/mm
```

Innerhalb der Ordner folgen die Namen der Protokolldateien einem ähnlichen Format:

```
account-id_waflogs_Region_web-acl-name_timestamp_hash.log.gz
```

Die in der Ordnerstruktur und im Namen der Protokolldatei verwendeten Zeitangaben entsprechen der Spezifikation des Zeitstempelformats YYYYMMddTHHmmZ.

Das folgende Beispiel zeigt eine Protokolldatei in einem Amazon-S3-Bucket für einen Bucket mit dem Namen DOC-EXAMPLE-BUCKET. Das AWS-Konto ist. 11111111111 Die Web-ACL ist TEST-WEBACL und die Region ist 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

Ihre Bucket-Namen für die AWS WAF Protokollierung müssen mit einem beliebigen Suffix beginnen `aws-waf-logs-` und können mit einem beliebigen Suffix enden.

Zum Veröffentlichen von Protokollen auf Amazon S3 sind Berechtigungen erforderlich

Die Konfiguration der Web-ACL-Datenverkehrsprotokollierung für einen Amazon-S3-Bucket erfordert die folgenden Berechtigungseinstellungen. Diese Berechtigungen werden für Sie festgelegt, wenn Sie eine der verwalteten AWS WAF -Richtlinien mit vollem Zugriff, `AWSWAFConsoleFullAccess` oder `AWSWAFFullAccess` verwenden. Wenn Sie den Zugriff auf Ihre Protokollierung und AWS WAF Ressourcen detaillierter verwalten möchten, können Sie diese Berechtigungen selbst festlegen. Informationen zur Verwaltung von Berechtigungen finden Sie unter [Zugriffsverwaltung für AWS Ressourcen](#) im IAM-Benutzerhandbuch. Informationen zu den AWS WAF verwalteten Richtlinien finden Sie unter [AWS verwaltete Richtlinien für AWS WAF](#).

Mit den folgenden Berechtigungen können Sie die Konfiguration der Web-ACL-Protokollierung ändern und die Protokollübertragung an Ihren Amazon-S3-Bucket konfigurieren. Diese Berechtigungen müssen an den Benutzer angehängt werden, den Sie zur Verwaltung von AWS WAF verwenden.

Note

Wenn Sie die unten aufgeführten Berechtigungen festlegen, werden in Ihren AWS CloudTrail Protokollen möglicherweise Fehler angezeigt, die darauf hinweisen, dass der Zugriff verweigert wurde, die Berechtigungen für die AWS WAF Protokollierung jedoch korrekt sind.

```
{
  "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"
  }
]
}

```

Wenn Aktionen für alle AWS Ressourcen zulässig sind, wird dies in der Richtlinie mit der "Resource" Einstellung von angegeben "*" . Das bedeutet, dass die Aktionen für alle AWS Ressourcen zulässig sind, die jede Aktion unterstützt. Die Aktion `wafv2:PutLoggingConfiguration` wird beispielsweise nur für `wafv2`-Protokollkonfigurationsressourcen unterstützt.

Standardmäßig sind Amazon-S3-Buckets und die darin enthaltenen Objekte privat. Nur der Bucket-Besitzer kann auf den Bucket und die darin gespeicherten Objekte zugreifen. Der Bucket-Besitzer

kann jedoch anderen Ressourcen und Benutzern Zugriffsberechtigungen gewähren, indem er eine Zugriffsrichtlinie schreibt.

Wenn der Benutzer, der das Protokoll erstellt, den Bucket besitzt, fügt der Service automatisch die folgende Richtlinie an den Bucket an, um dem Protokoll die Berechtigung zum Veröffentlichen von Protokollen darin zu erteilen.

```
{
  "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

Ihre Bucket-Namen für die AWS WAF Protokollierung müssen mit einem beliebigen Suffix beginnen `aws-waf-logs-` und können mit einem beliebigen Suffix enden.

Wenn der Benutzer, der das Protokoll erstellt, nicht Eigentümer des Buckets ist, hat er keine `GetBucketPolicy-` und `PutBucketPolicy-`Berechtigungen für den Bucket und das Protokoll kann nicht erstellt werden. In diesem Fall muss der Bucket-Eigentümer dem Bucket die vorherige Richtlinie manuell hinzufügen und die AWS-Konto -ID des Erstellers des Protokolls angeben. Weitere Informationen erhalten Sie unter [Wie füge ich einen S3 Bucket hinzu?](#) im Benutzerhandbuch zu Amazon Simple Storage Service. Wenn der Bucket Protokolle von mehreren Konten erhält, fügen Sie der `AWSLogDeliveryWrite`-Richtlinienanweisung für jedes Konto einen `Resource`-Elementeintrag hinzu.

Die folgende Bucket-Richtlinie ermöglicht beispielsweise die Veröffentlichung von Logs AWS-Konto 111122223333 in einem Bucket mit dem Namen `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:*"]
            }
        }
    }
]
}

```

Berechtigungen für die Verwendung AWS Key Management Service mit einem KMS-Schlüssel

Wenn Ihr Protokollierungsziel serverseitige Verschlüsselung mit Schlüsseln verwendet, die in AWS Key Management Service (SSE-KMS) gespeichert sind, und Sie einen vom Kunden verwalteten Schlüssel (KMS-Schlüssel) verwenden, müssen Sie die AWS WAF Erlaubnis zur Verwendung Ihres KMS-Schlüssels erteilen. Dazu fügen Sie dem KMS-Schlüssel für das von Ihnen gewählte Ziel eine Schlüsselrichtlinie hinzu. Auf diese Weise kann die AWS WAF Protokollierung Ihre Protokolldateien an Ihr Ziel schreiben.

Fügen Sie Ihrem KMS-Schlüssel die folgende Schlüsselrichtlinie hinzu, damit Sie AWS WAF sich bei Ihrem Amazon S3-Bucket anmelden können.

```

{
    "Sid": "Allow AWS WAF to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    }
}

```



```
    ]  
  },  
  "Action": "kms:GenerateDataKey*",  
  "Resource": "*" }  
}
```

Für den Zugriff auf Amazon S3 S3-Protokolldateien sind Berechtigungen erforderlich

Amazon S3 verwendet Zugriffskontrolllisten (ACLs), um den Zugriff auf die von einem AWS WAF Protokoll erstellten Protokolldateien zu verwalten. Standardmäßig hat der Bucket-Eigentümer FULL_CONTROL-Berechtigungen für jede Protokolldatei. Der Protokollbereitstellungseigentümer hat keine Berechtigungen, wenn er nicht gleichzeitig der Bucket-Eigentümer ist. Das Konto für die Protokollbereitstellung hat READ- und WRITE-Berechtigungen. Weitere Informationen finden Sie unter [Zugriffskontrollliste \(ACL\) – Übersicht](#) im Benutzerhandbuch zu Amazon Simple Storage Service.

Amazon Data Firehose

Dieser Abschnitt enthält Informationen zum Senden Ihrer Web-ACL-Traffic-Logs an eine Amazon Data Firehose.

Note

Die Kosten für die Protokollierung werden zusätzlich zu den Kosten für die Nutzung von AWS WAF berechnet. Weitere Informationen finden Sie unter [Preise für die Protokollierung von Web-ACL-Datenverkehrsinformationen](#).

Um Protokolle an Amazon Data Firehose zu senden, senden Sie Protokolle von Ihrer Web-ACL an eine Amazon Data Firehose mit einem konfigurierten Speicherziel. Nachdem Sie die Protokollierung aktiviert haben AWS WAF , werden Protokolle über den HTTPS-Endpunkt von Firehose an Ihr Speicherziel gesendet.

Ein AWS WAF Protokoll entspricht einem Firehose-Datensatz. Wenn Sie in der Regel 10.000 Anfragen pro Sekunde erhalten und vollständige Protokolle aktivieren, sollten Sie in Firehose eine Einstellung von 10.000 Datensätzen pro Sekunde haben. Wenn Sie Firehose nicht richtig konfigurieren, AWS WAF werden nicht alle Protokolle aufgezeichnet. Weitere Informationen finden Sie unter [Amazon Kinesis Data Firehose-Kontingente](#).

Informationen dazu, wie Sie eine Amazon Data Firehose erstellen und Ihre gespeicherten Protokolle überprüfen können, finden Sie unter [Was ist Amazon Data Firehose?](#)

Informationen zur Erstellung Ihres Lieferdatenstroms finden Sie unter [Erstellen eines Amazon Data Firehose-Lieferdatenstroms](#).

Konfiguration eines Amazon Data Firehose-Lieferdatenstroms für Ihre Web-ACL

Konfigurieren Sie wie folgt einen Amazon Firehose Firehose-Lieferstream für Ihre Web-ACL.

- Erstellen Sie ihn mit demselben Konto, das Sie für die Verwaltung der Web-ACL verwenden.
- Erstellen Sie ihn in der gleichen Region wie die Web-ACL. Wenn Sie Logs für Amazon erfassen CloudFront, erstellen Sie die Firehose in der Region USA Ost (Nord-Virginia), `us-east-1`.
- Geben Sie dem Data Firehose einen Namen, der mit dem Präfix `aws-waf-logs-` beginnt. z. B. `aws-waf-logs-us-east-2-analytics`.
- Konfigurieren Sie ihn für Direct Put, sodass Anwendungen direkt auf den Bereitstellungsstrom zugreifen können. Wählen Sie in der Amazon Data Firehose-Konsole für die Einstellung Delivery Stream Source die Option Direct PUT oder andere Quellen aus. Legen Sie über die API die Eigenschaft `DeliveryStreamType` des Bereitstellungsstroms auf `DirectPut` fest.

Note

Verwenden Sie keinen `Kinesis stream` als Ihre Quelle.

Zum Veröffentlichen von Protokollen in einer Amazon Data Firehose sind Berechtigungen erforderlich

Informationen zu den für Ihre Kinesis-Data-Firehose-Konfiguration erforderlichen Berechtigungen finden Sie unter [Controlling Access with Amazon Kinesis Data Firehose](#) (Zugriff mit Amazon Kinesis Data Firehose steuern).

Sie müssen über die folgenden Berechtigungen verfügen, um die Web-ACL-Protokollierung mit einer Amazon Data Firehose erfolgreich zu aktivieren.

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

Weitere Informationen zu serviceverknüpften Rollen und zur `iam:CreateServiceLinkedRole`-Berechtigung finden Sie unter [Verwenden von serviceverknüpften Rollen für AWS WAF](#).

Verwalten der Protokollierung für eine Web-ACL

Sie können die Protokollierung für eine Web-ACL jederzeit aktivieren oder deaktivieren.

Note

Die Kosten für die Protokollierung werden zusätzlich zu den Kosten für die Nutzung von AWS WAF berechnet. Weitere Informationen finden Sie unter [Preise für die Protokollierung von Web-ACL-Datenverkehrsdaten](#).

In der Logging-Konfiguration für Ihre Web-ACL können Sie anpassen, was AWS WAF an die Logs gesendet wird.

- Schwärzung von Feldern — Sie können die folgenden Felder aus den Protokolldatensätzen für die Regeln, die die entsprechenden Übereinstimmungseinstellungen verwenden, schwärzen: URI-Pfad, Abfragezeichenfolge, Einzelner Header und HTTP-Methode. Die unkenntlich gemachten Felder werden in den Protokollen als REDACTED angezeigt. Wenn Sie beispielsweise das Feld „Abfragezeichenfolge“ in den Protokollen unkenntlich machen, wird es wie bei allen Regeln aufgeführt, die die REDACTED Komponenteneinstellung „Abfragezeichenfolge abgleichen“ verwenden. Schwärzen bezieht sich nur auf die Anforderungskomponente, die Sie in der Regel für den Abgleich angeben. Daher gilt die Schwärzung der Komponente Einzelner Header nicht für Regeln, die auf Kopfzeilen übereinstimmen. Eine Liste der Protokollfelder finden Sie unter [Protokollfelder](#).

Note

Diese Einstellung hat keine Auswirkungen auf das Sampling von Anfragen. Beim Anforderungssampling können Felder nur ausgeschlossen werden, indem das Sampling für die Web-ACL deaktiviert wird.

- Filtern von Protokollen: Sie können Filter hinzufügen, um anzugeben, welche Webanforderungen in den Protokollen gespeichert und welche gelöscht werden. Sie filtern nach den Einstellungen, die bei der Auswertung von Webanfragen AWS WAF gelten. Sie können nach den folgenden Einstellungen filtern:
 - Vollqualifiziertes Label — Vollqualifizierte Labels haben ein Präfix, optionale Namespaces und einen Labelnamen. Das Präfix identifiziert die Regelgruppe oder den Web-ACL-Kontext der


Regel, die die Beschriftung hinzugefügt hat. Weitere Informationen zu Bezeichnungen finden Sie unter [AWS WAF Labels auf Webanfragen](#).

- **Regelaktion** — Sie können nach jeder normalen Regelaktionseinstellung und auch nach der älteren Option zum EXCLUDED_AS_COUNT Überschreiben von Regelgruppenregeln filtern. Weitere Informationen zu Einstellungen für Regelaktionen finden Sie unter [Regelaktion](#). Informationen zu aktuellen und älteren Regelaktionsüberschreibungen für Regelgruppenregeln finden Sie unter [Aktionsüberschreibungen in Regelgruppen](#).
- Die normalen Regelaktionsfilter gelten für Aktionen, die in Regeln konfiguriert sind, sowie für Aktionen, die mithilfe der aktuellen Option zum Überschreiben einer Regelgruppenregelaktion konfiguriert wurden.
- Der EXCLUDED_AS_COUNT Protokollfilter überschneidet sich mit dem Count Aktionsprotokollfilter. EXCLUDED_AS_COUNT filtert sowohl die aktuellen als auch die älteren Optionen zum Überschreiben einer Regelgruppenregelaktion auf. Count

Aktivieren der Protokollierung für eine Web-ACL


Für dieses Verfahren ist ein konfiguriertes Protokollierungsziel erforderlich. Informationen über Ihre Zielauswahl und die jeweiligen Anforderungen finden Sie unter [AWS WAF Ziele protokollieren](#).

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich Web ACLs aus.
3. Wählen Sie die Web-ACL aus, für die Sie die Protokollierung aktivieren möchten. Die Konsole führt Sie zur Beschreibung der Web-ACL, wo Sie sie bearbeiten können.
4. Klicken Sie auf der Registerkarte Logging (Protokollieren) auf Enable logging (Protokollieren aktivieren).
5. Wählen Sie den Protokolliererzieltyp und dann das konfigurierte Protokollierungsziel aus. Sie müssen ein Protokollierungsziel auswählen, dessen Name mit `aws-waf-logs-` beginnt.
6. (Optional) Wenn Sie nicht möchten, dass einige Felder in den Protokollen enthalten sind, redigieren Sie sie. Wählen Sie das Feld aus, das unkenntlich gemacht werden soll, und klicken Sie dann auf Add (Hinzufügen). Wiederholen Sie diesen Vorgang nach Bedarf, um zusätzliche Felder unkenntlich zu machen.

 Note

Diese Einstellung hat keine Auswirkungen auf das Sampling von Anfragen. Beim Anforderungssampling können Felder nur ausgeschlossen werden, indem das Sampling für die Web-ACL deaktiviert wird.

7. (Optional) Wenn Sie nicht alle Anforderungen an die Protokolle senden möchten, fügen Sie Filterkriterien und -verhalten hinzu. Wählen Sie unter Filter logs (Protokolle filtern) für jeden Filter, den Sie anwenden möchten, Add filter (Filter hinzufügen) aus. Wählen Sie dann Ihre Filterkriterien und geben Sie an, ob Sie Anforderungen, die den Kriterien entsprechen, beibehalten oder löschen möchten. Wenn Sie mit dem Hinzufügen von Filtern fertig sind, ändern Sie bei Bedarf das Standardprotokollierungsverhalten.
8. Wählen Sie Enable logging (Protokollierung aktivieren) aus.

 Note

Wenn Sie die Protokollierung erfolgreich aktivieren, AWS WAF wird eine serviceverknüpfte Rolle mit den erforderlichen Berechtigungen zum Schreiben von Protokollen an das Protokollierungsziel erstellt. Weitere Informationen finden Sie unter [Verwenden von serviceverknüpften Rollen für AWS WAF](#).

Deaktivieren der Protokollierung für eine Web-ACL

1. Wählen Sie im Navigationsbereich Web ACLs aus.
2. Wählen Sie die Web-ACL aus, für die Sie die Protokollierung deaktivieren möchten. Die Konsole führt Sie zur Beschreibung der Web-ACL, wo Sie sie bearbeiten können.
3. Klicken Sie auf der Registerkarte Logging (Protokollieren) auf Disable logging (Protokollieren deaktivieren).
4. Wählen Sie im Dialogfeld Disable logging (Protokollieren deaktivieren).

Protokollfelder

In der folgenden Liste werden die wichtigsten Protokollfelder beschrieben.

action

Die abschließende Aktion, die für die Anfrage AWS WAF galt. Dies bedeutet entweder „Zulassen“, „Blockieren“, „CAPTCHA“ oder „Abfordern“. Die Challenge Aktionen CAPTCHA und werden beendet, wenn die Webanforderung kein gültiges Token enthält.

args

Die Abfragezeichenfolge.

captchaResponse

Der CAPTCHA-Aktionsstatus für die Anfrage, der ausgefüllt wird, wenn eine CAPTCHA Aktion auf die Anfrage angewendet wird. Dieses Feld wird für jede CAPTCHA Aktion aufgefüllt, unabhängig davon, ob sie beendet oder nicht beendet wird. Wenn die CAPTCHA Aktion auf eine Anfrage mehrfach angewendet wurde, wird dieses Feld ab dem Zeitpunkt gefüllt, zu dem die Aktion das letzte Mal angewendet wurde.

Die CAPTCHA Aktion beendet die Überprüfung von Webanfragen, wenn die Anfrage entweder kein Token enthält oder das Token ungültig oder abgelaufen ist. Wenn die CAPTCHA Aktion beendet wird, enthält dieses Feld einen Antwortcode und einen Grund für den Fehler. Wenn die Aktion nicht beendet wird, enthält dieses Feld einen Lösungszeitstempel. Um zwischen einer abschließenden und einer nicht beendenden Aktion zu unterscheiden, können Sie in diesem Feld nach einem nicht leeren Attribut filtern. `failureReason`

ChallengeResponse

Der Status der Challenge-Aktion für die Anfrage, der aufgefüllt wird, wenn eine Challenge Aktion auf die Anfrage angewendet wird. Dieses Feld wird für jede Challenge Aktion aufgefüllt, unabhängig davon, ob sie beendet oder nicht beendet wird. Wenn die Challenge Aktion auf eine Anfrage mehrfach angewendet wurde, wird dieses Feld ab dem Zeitpunkt gefüllt, zu dem die Aktion das letzte Mal angewendet wurde.

Die Challenge Aktion beendet die Überprüfung von Webanfragen, wenn die Anfrage entweder kein Token enthält oder das Token ungültig oder abgelaufen ist. Wenn die Challenge Aktion beendet wird, enthält dieses Feld einen Antwortcode und einen Grund für den Fehler. Wenn die Aktion nicht beendet wird, enthält dieses Feld einen Lösungszeitstempel. Um zwischen einer abschließenden und einer nicht beendenden Aktion zu unterscheiden, können Sie in diesem Feld nach einem nicht leeren Attribut filtern. `failureReason`

clientIp

Die IP-Adresse des Clients, der die Anforderung sendet.

country

Das Quellland der Anforderung. Wenn AWS WAF das Herkunftsland nicht bestimmt werden kann, wird dieses Feld auf gesetzt. -

excludedRules

Wird nur für Regelgruppenregeln verwendet. Die Liste der Regeln in der Regelgruppe, die von Ihnen ausgeschlossen wurden. Die Aktion für diese Regeln ist auf eingestelltCount.

Wenn Sie mit der Aktionsoption „Regel überschreiben“ eine Regel so überschreiben, dass sie zählt, werden Treffer hier nicht aufgeführt. Sie werden als Aktionspaare action und aufgeführtoverriddenAction.

exclusionType

Ein Typ, der angibt, dass die ausgeschlossene Regel die Aktion hatCount.

ruleId

Die ID der Regel innerhalb der Regelgruppe, die ausgeschlossen ist.

formatVersion

Die Formatversion für das Protokoll.

Header

Die Liste der Header.

httpMethod

Die HTTP-Methode in der Anforderung.

httpRequest

Die Metadaten zu der Anforderung.

httpSourceId

Die ID der zugehörigen Ressource:

- Für eine CloudFront Amazon-Distribution ist die ID *distribution-id* in der ARN-Syntax wie folgt:

```
arn:partitioncloudfront::account-id:distribution/distribution-id
```

- Für einen Application Load Balancer entspricht die ID *load-balancer-id* in der ARN-Syntax:

```
arn:partition:elasticloadbalancing:region:account-id:loadbalancer/  
app/load-balancer-name/load-balancer-id
```

- Für eine Amazon API Gateway Gateway-REST-API entspricht die ID *api-id* in der ARN-Syntax:

```
arn:partition:apigateway:region::/restapis/api-id/stages/stage-name
```

- Für eine AWS AppSync GraphQL-API ist die ID *GraphQLApiId* in der ARN-Syntax:

```
arn:partition:appsync:region:account-id:apis/GraphQLApiId
```

- Für einen Amazon Cognito Cognito-Benutzerpool ist die ID *user-pool-id* in der ARN-Syntax:

```
arn:partition:cognito-idp:region:account-id:userpool/user-pool-id
```

- Für einen AWS App Runner Dienst ist die ID *apprunner-service-id* in der ARN-Syntax:

```
arn:partition:apprunner:region:account-id:service/apprunner-service-  
name/apprunner-service-id
```

httpSourceName

Die Quelle der Anforderung. Mögliche Werte: CF für Amazon CloudFront, APIGW für Amazon API Gateway, ALB für Application Load Balancer, APPSYNC für AWS AppSync, COGNITOIDP für Amazon Cognito, APPRUNNER für App Runner und VERIFIED_ACCESS für Verified Access.

httpVersion

Die HTTP-Version.

JA3-Fingerabdruck

Der JA3-Fingerabdruck der Anfrage. Der JA3-Fingerabdruck ist ein 32-stelliger Hash, der vom TLS-Client-Hello einer eingehenden Anfrage abgeleitet wird. Dieser Fingerabdruck dient als eindeutige Kennung für die TLS-Konfiguration des Clients. AWS WAF berechnet und protokolliert diesen Fingerabdruck für jede Anfrage, die genügend TLS-Client-Hello-Informationen für die Berechnung enthält.

Sie geben diesen Wert an, wenn Sie in Ihren Web-ACL-Regeln einen JA3-Fingerabdruckabgleich konfigurieren. Informationen zum Erstellen eines Abgleichs mit dem JA3-Fingerabdruck finden Sie [JA3-Fingerabdruck](#) in der Anweisung [Anforderungskomponentenoptionen](#) Für eine Regel.

labels

Die Bezeichnungen in der Webanforderung. Diese Bezeichnungen wurden durch Regeln zugewiesen, die zur Auswertung der Anfrage verwendet wurden. AWS WAF protokolliert die ersten 100 Labels.

nonTerminatingMatchingRegeln

Die Liste der nicht abschließenden Regeln, die der Anfrage entsprachen. Jeder Eintrag in der Liste enthält die folgenden Informationen.

action

Die Aktion, die AWS WAF auf die Anfrage angewendet wurde. Dies gibt entweder Anzahl, CAPTCHA oder Herausforderung an. Die CAPTCHA und Challenge enden nicht, wenn die Webanforderung ein gültiges Token enthält.

ruleId

Die ID der Regel, die mit der Anforderung übereinstimmt und nicht beendend war.

ruleMatchDetails

Detaillierte Informationen zur Regel, die mit der Anforderung übereingestimmt hat. Dieses Feld wird nur für SQL-Injection und Cross-Site Scripting (XSS)-Übereinstimmungsregelungen ausgefüllt. Eine Vergleichsregel erfordert möglicherweise eine Übereinstimmung mit mehr als einem Prüfkriterium. Daher werden diese Übereinstimmungsdetails als eine Reihe von Übereinstimmungskriterien bereitgestellt.

Alle zusätzlichen Informationen, die für jede Regel bereitgestellt werden, hängen von Faktoren wie der Regelkonfiguration, der Art der Regelübereinstimmung und den Details der Übereinstimmung ab. Bei Regeln mit der Challenge Aktion „CAPTCHAoder“ `challengeResponse` wird beispielsweise das „`captchaResponseoder`“ aufgeführt. Wenn sich die entsprechende Regel in einer Regelgruppe befindet und Sie die zugehörige konfigurierte Regelaktion außer Kraft gesetzt haben, wird die konfigurierte Aktion in bereitgestellt. `overriddenAction`

oversizeFields

Die Liste der Felder in der Webanforderung, die von der Web-ACL geprüft wurden und deren AWS WAF Inspektionslimit überschritten wurde. Wenn ein Feld übergroß ist, aber von der Web-ACL nicht überprüft wird, wird es hier nicht aufgeführt.

Diese Liste kann null oder mehr der folgenden Werte enthalten: `REQUEST_BODY`, `REQUEST_JSON_BODY`, `REQUEST_HEADERS` und `REQUEST_COOKIES`. Weitere Informationen zu

übergroßen Feldern finden Sie unter [Umgang mit übergroßen Webanforderungskomponenten in AWS WAF](#).

rateBasedRuleListe

Die Liste der ratenbasierten Regeln, die auf die Anforderung reagiert haben. Weitere Informationen über ratenbasierte Regeln finden Sie unter [Ratenbasierte Regelnweisung](#).

rateBasedRuleID

Die ID der ratenbasierten Regel, die auf die Anforderung reagiert hat. Wenn die Anforderung hierdurch beendet wurde, ist die ID für `rateBasedRuleId` mit der ID für `terminatingRuleId` identisch.

rateBasedRuleName

Der Name der ratenbasierten Regel, die auf die Anforderung reagiert hat.

limitKey

Der Aggregationstyp, den die Regel verwendet. Mögliche Werte sind `IP` für den Ursprung der Webanfrage, `FORWARDED_IP` für eine IP, die in einem Header der Anfrage weitergeleitet wird, `CUSTOMKEYS` für benutzerdefinierte Aggregatschlüsseleinstellungen und `CONSTANT` für das Zusammenzählen aller Anfragen ohne Aggregation.

limitValue

Wird nur bei der Ratenbegrenzung durch einen einzigen IP-Adresstyp verwendet. Wenn eine Anforderung eine ungültige IP-Adresse enthält, ist der `limitvalue` `INVALID`.

maxRateAllowed

Die maximale Anzahl von Anfragen, die im angegebenen Zeitfenster für eine bestimmte Aggregationsinstanz zulässig sind. Die Aggregationsinstanz wird durch die `limitKey` und alle zusätzlichen Schlüsselpezifikationen definiert, die Sie in der ratenbasierten Regelkonfiguration angegeben haben.

evaluationWindowSec

Die Zeit, die in der Anfrage AWS WAF enthalten ist, wird in Sekunden gezählt.

Benutzerdefinierte Werte

Eindeutige Werte, die durch die ratenbasierte Regel in der Anfrage identifiziert werden. Bei Zeichenkettenwerten geben die Protokolle die ersten 32 Zeichen des Zeichenfolgenwerts aus. Je nach Schlüsseltyp können diese Werte nur für einen Schlüssel gelten, z. B. für eine

HTTP-Methode oder eine Abfragezeichenfolge, oder sie können für einen Schlüssel und einen Namen gelten, z. B. für den Header und den Headernamen.

requestHeadersInserted

Die Liste der Kopfzeilen, die für die benutzerdefinierte Bearbeitung von Anforderungen eingefügt werden.

requestId

Die ID der Anforderung, die vom zugrunde liegenden Host-Service generiert wird. Bei Application Load Balancer ist dies die Ablaufverfolgungs-ID. Bei allen anderen ist dies die Anforderungs-ID.

responseCodeSent

Der Antwortcode, der mit einer benutzerdefinierten Antwort gesendet wird.

ruleGroupId

Die ID der Regelgruppe. Wenn die Regel die Anforderung blockiert hat, ist die ID für `ruleGroupID` mit der ID für `terminatingRuleId` identisch.

ruleGroupList

Die Liste der Regelgruppen, die auf diese Anfrage reagiert haben, mit Übereinstimmungsinformationen.

terminatingRule

Die Regel, die die Anforderung beendet. Falls diese vorhanden ist, enthält sie die folgenden Informationen.

action

Die abschließende Aktion, die AWS WAF auf die Anfrage angewendet wurde. Dies bedeutet entweder „Zulassen“, „Blockieren“, „CAPTCHA“ oder „Abfordern“. Die Challenge Aktionen CAPTCHA und werden beendet, wenn die Webanforderung kein gültiges Token enthält.

ruleId

Die ID der Regel, die der Anfrage entsprach.

ruleMatchDetails

Detaillierte Informationen zur Regel, die mit der Anforderung übereingestimmt hat. Dieses Feld wird nur für SQL-Injection und Cross-Site Scripting (XSS)-Übereinstimmungsregelungen ausgefüllt. Eine Abgleichsregel erfordert

möglicherweise eine Übereinstimmung mit mehr als einem Prüfkriterium. Daher werden diese Übereinstimmungsdetails als eine Reihe von Übereinstimmungskriterien bereitgestellt.

Alle zusätzlichen Informationen, die für jede Regel bereitgestellt werden, hängen von Faktoren wie der Regelkonfiguration, der Art der Regelübereinstimmung und den Details der Übereinstimmung ab. Bei Regeln mit der Challenge Aktion „CAPTCHAoder“ challengeResponse wird beispielsweise das „captchaResponseoder“ aufgeführt. Wenn sich die entsprechende Regel in einer Regelgruppe befindet und Sie die zugehörige konfigurierte Regelaktion außer Kraft gesetzt haben, wird die konfigurierte Aktion in bereitgestellt. overriddenAction

terminatingRuleId

Die ID der Regel, die die Anforderung beendet. Wenn nichts zur Beendigung der Anforderung führt, ist der Wert Default_Action.

terminatingRuleMatchEinzelheiten

Detaillierte Informationen zur Beendigungsregel, die mit der Anforderung übereingestimmt hat. Eine Beendigungsregel verfügt über eine Aktion, die den Inspektionsprozess für eine Webanforderung beendet. Zu den möglichen Aktionen für eine abschließende Regel gehörenAllow, BlockCAPTCHA, undChallenge. Bei der Überprüfung einer Webanforderung wird die Prüfung bei der ersten Regel, die der Anforderung entspricht und die eine abschließende Aktion enthält, AWS WAF beendet und die Aktion angewendet. Die Webanfrage kann zusätzlich zu der Bedrohung, die im Protokoll für die entsprechende Beendigungsregel aufgeführt ist, weitere Bedrohungen enthalten.

Dies wird nur für SQL-Injection und Cross-Site Scripting (XSS) - Übereinstimmungsregelanweisungen aufgefüllt. Die Vergleichsregel erfordert möglicherweise eine Übereinstimmung mit mehr als einem Prüfkriterium. Daher werden diese Übereinstimmungsdetails als eine Reihe von Übereinstimmungskriterien bereitgestellt.

terminatingRuleType

Der Typ der Regel, die die Anforderung beendet. Mögliche Werte: RATE_BASED, REGULAR, GROUP und MANAGED_RULE_GROUP.

Zeitstempel

Der Zeitstempel in Millisekunden.

uri

Der URI der Anforderung.

webaclId

Die GUID der Web-ACL.

Beispiele protokollieren

Example Ratenbasierte Regel 1: Regelkonfiguration mit einem Schlüssel, eingestellt auf

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 Ratenbasierte Regel 1: Protokolleintrag für eine Anfrage, die durch eine ratenbasierte Regel blockiert wurde

```
{
  "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 Ratenbasierte Regel 2: Regelkonfiguration mit zwei Schlüsseln, eingestellt auf und 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 Ratenbasierte Regel 2: Protokolleintrag für eine Anfrage, die durch eine ratenbasierte Regel blockiert wurde

```

{
  "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":"2311byn8v3.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": "EdzmlH50CGYF1vQ="
  }
}

```

Example Protokollausgabe für eine Regel, die bei der SQLi-Erkennung ausgelöst wurde (beendend)

```

{
  "timestamp": 1576280412771,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/STMTTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
  "terminatingRuleId": "STMTTest_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 Protokollausgabe für eine Regel, die bei SQLi-Erkennung ausgelöst wurde (nicht beendend)

```

{
  "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 Protokollausgabe für mehrere Regeln, die innerhalb einer Regelgruppe ausgelöst wurden (RuleA-XSS ist beendend und Rule-B ist nicht beendend)

```
{
  "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/c051b698-1f11-4m41-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 Protokollausgabe für eine Regel, die die Prüfung des Anforderungstextes mit Inhaltstyp JSON ausgelöst hat

AWS WAF meldet derzeit den Standort für die JSON-Bodyinspektion als. UNKNOWN

```

{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:123456789012:regional/webacl/test/111",
    "terminatingRuleId": "STMTTest_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 Protokollausgabe für eine CAPTCHA-Regel anhand einer Webanforderung mit einem gültigen, noch nicht abgelaufenen CAPTCHA-Token

Die folgende Protokollliste bezieht sich auf eine Webanforderung, die mit einer Regel mit CAPTCHA-Aktion übereinstimmt. Die Webanforderung hat ein gültiges und nicht abgelaufenes CAPTCHA-Token und wird nur von als CAPTCHA-Übereinstimmung vermerkt, ähnlich dem Verhalten für die Aktion. AWS WAFCount Dieser CAPTCHA-Abgleich ist unter vermerkt. `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:t9wvxw042wva7E2Y6lgud/
bS6YG0CJkVAJqaRqDZ140ythKW0Zj9wKB2081SkYDRqf1y0NcVBFo5u0eYi0tvT4rtQCXsu
+KanAardW8go4QSLw4yoED59lgV7oAhGyCalAzE7ra29j+RvvZPsQyoQuDCrtoY/TvQyMTXIXzGPDC/rKBbg=="
  }
],
"uri": "/pen-test/pets",
"args": "",
"httpVersion": "HTTP/1.1",
"httpMethod": "GET",
"requestId": "GINMHHUgoAMFjug="
}
}

```

Example Protokollausgabe für eine CAPTCHA-Regel für eine Webanfrage, die kein CAPTCHA-Token hat

Die folgende Protokolliste bezieht sich auf eine Webanforderung, die mit einer Regel mit CAPTCHA-Aktion übereinstimmt. Die Webanfrage hatte kein CAPTCHA-Token und wurde von blockiert. 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": "GINKHEssoAMFsrq=",  
  },  
  "captchaResponse": {  
    "responseCode": 405,  
    "solveTimestamp": 0,  
    "failureReason": "TOKEN_MISSING"  
  }  
}
```

Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen

Wir empfehlen Ihnen, alle Änderungen an Ihrer AWS WAF Web-ACL zu testen und zu optimieren, bevor Sie sie auf den Traffic Ihrer Website oder Webanwendung anwenden.

Risiken rund um Produktionsdatenverkehr

Bevor Sie Ihre Web-ACL-Implementierung für den Produktionsdatenverkehr einsetzen, testen und optimieren Sie sie in einer Staging- oder Testumgebung, bis Sie mit den möglichen Auswirkungen auf Ihren Traffic zufrieden sind. Testen und optimieren Sie dann die Regeln im Zählmodus mit Ihrem Produktionsdatenverkehr, bevor Sie sie aktivieren.

Dieser Abschnitt enthält Anleitungen zum Testen und Optimieren Ihrer AWS WAF Web-ACLs, Regeln, Regelgruppen, IP-Sätze und Regex-Mustersätze.

Dieser Abschnitt enthält auch allgemeine Anleitungen zum Testen der Verwendung von Regelgruppen, die von einer anderen Person verwaltet werden. Dazu gehören Regelgruppen für AWS verwaltete Regeln, AWS Marketplace verwaltete Regelgruppen und Regelgruppen, die von einem anderen Konto für Sie gemeinsam genutzt werden. Folgen Sie für diese Regelgruppen auch den Anweisungen, die Sie vom Regelgruppenanbieter erhalten.

- Informationen zur Regelgruppe „AWS Verwaltete Regeln von Bot Control“ finden Sie auch unter [Testen und Bereitstellen von AWS WAF Bot Control](#).
- Informationen zur Regelgruppe „AWS Verwaltete Regeln zur Verhinderung von Kontoübernahmen“ finden Sie auch unter [Testen und Bereitstellen von ATP](#).

- Informationen zur Regelgruppe „AWS Verwaltete Regeln zur Verhinderung von Betrug bei der Kontoerstellung“ finden Sie auch unter [Testen und Bereitstellen von ACFP](#).

Vorübergehende Inkonsistenzen bei Aktualisierungen

Wenn Sie eine Web-ACL oder andere AWS WAF Ressourcen erstellen oder ändern, dauert es nicht lange, bis die Änderungen in allen Bereichen, in denen die Ressourcen gespeichert sind, übernommen werden. Die Übertragungszeit kann zwischen einigen Sekunden und mehreren Minuten liegen.

Im Folgenden finden Sie Beispiele für temporäre Inkonsistenzen, die Ihnen bei der Übertragung von Änderungen möglicherweise auffallen:

- Wenn Sie nach der Erstellung einer Web-ACL versuchen, sie einer Ressource zuzuordnen, wird möglicherweise eine Ausnahme angezeigt, die darauf hinweist, dass die Web-ACL nicht verfügbar ist.
- Nachdem Sie einer Web-ACL eine Regelgruppe hinzugefügt haben, gelten die neuen Regelgruppenregeln möglicherweise in einem Bereich, in dem die Web-ACL verwendet wird, und nicht in einem anderen.
- Nachdem Sie eine Regelaktionseinstellung geändert haben, sehen Sie möglicherweise an einigen Stellen die alte Aktion und an anderen die neue Aktion.
- Nachdem Sie einem IP-Set, das in einer Sperrregel verwendet wird, eine IP-Adresse hinzugefügt haben, wird die neue Adresse möglicherweise in einem Bereich blockiert, während sie in einem anderen weiterhin zulässig ist.

Testen und Optimieren von Schritten auf hoher Ebene

Dieser Abschnitt enthält eine Checkliste mit den Schritten zum Testen von Änderungen an Ihrer Web-ACL, einschließlich aller Regeln oder Regelgruppen, die sie verwendet.

Note

Um den Anleitungen in diesem Abschnitt folgen zu können, müssen Sie wissen, wie AWS WAF Schutzmaßnahmen wie Web-ACLs, Regeln und Regelgruppen erstellt und verwaltet werden. Diese Informationen wurden in früheren Abschnitten dieses Handbuchs behandelt.

Um Ihre Web-ACL zu testen und zu optimieren

Führen Sie diese Schritte zuerst in einer Testumgebung und dann in der Produktion aus.

1. Bereiten Sie sich auf das Testen vor

Bereiten Sie Ihre Überwachungsumgebung vor, schalten Sie Ihre neuen AWS WAF Schutzmaßnahmen zum Testen in den Zählmodus und erstellen Sie alle benötigten Ressourcenzuordnungen.

Siehe [Vorbereitung für das Testen](#).

2. Überwachen und optimieren Sie Test- und Produktionsumgebungen

Überwachen und passen Sie Ihre AWS WAF Schutzmaßnahmen zunächst in einer Test- oder Staging-Umgebung und dann in der Produktion an, bis Sie überzeugt sind, dass sie den Datenverkehr so bewältigen können, wie Sie es benötigen.

Siehe [Überwachung und Tuning](#).

3. Aktivieren Sie Ihre Schutzmaßnahmen in der Produktion

Wenn Sie mit Ihren Testschutzmaßnahmen zufrieden sind, schalten Sie sie in den Produktionsmodus um, bereinigen Sie alle unnötigen Testartefakte und setzen Sie die Überwachung fort.

Siehe [Aktivierung Ihres Schutzes in der Produktion](#).

Nachdem Sie die Implementierung Ihrer Änderungen abgeschlossen haben, überwachen Sie weiterhin Ihren Web-Traffic und Ihre Schutzmaßnahmen in der Produktion, um sicherzustellen, dass sie wie gewünscht funktionieren. Die Muster des Webverkehrs können sich im Laufe der Zeit ändern, sodass Sie die Schutzmaßnahmen möglicherweise gelegentlich anpassen müssen.

Vorbereitung für das Testen

In diesem Abschnitt wird beschrieben, wie Sie sich einrichten, um Ihre AWS WAF Schutzmaßnahmen zu testen und zu optimieren.

Note

Um den Anleitungen in diesem Abschnitt folgen zu können, müssen Sie allgemein wissen, wie AWS WAF Schutzmaßnahmen wie Web-ACLs, Regeln und Regelgruppen erstellt und

verwaltet werden. Diese Informationen wurden in früheren Abschnitten dieses Handbuchs behandelt.

Um sich auf den Test vorzubereiten

1. Web-ACL-Protokollierung, CloudWatch Amazon-Metriken und Webanforderungssampling für die Web-ACL aktivieren

Verwenden Sie Protokollierung, Metriken und Sampling, um die Interaktion der Web-ACL-Regeln mit Ihrem Web-Traffic zu überwachen.

- Protokollierung — Sie können so konfigurieren AWS WAF , dass die Webanfragen, die eine Web-ACL auswertet, protokolliert werden. Sie können Protokolle an CloudWatch Protokolle, einen Amazon S3 S3-Bucket oder eine Amazon Data Firehose senden. Sie können Felder unkenntlich machen und Filter anwenden. Weitere Informationen finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).
- CloudWatch Amazon-Metriken — Geben Sie in Ihrer Web-ACL-Konfiguration Metrikspezifikationen für alles an, was Sie überwachen möchten. Sie können sich Metriken über die CloudWatch Konsolen AWS WAF und anzeigen lassen. Weitere Informationen finden Sie unter [Überwachung mit Amazon CloudWatch](#).
- Stichprobe von Webanfragen — Sie können sich eine Stichprobe aller Webanfragen ansehen, die Ihre Web-ACL auswertet. Informationen zum Sampling von Webanforderungen finden Sie unter [Anzeigen einer Stichprobe von Webanforderungen](#).

2. Stellen Sie Ihre Schutzmaßnahmen auf Modus Count

Schalten Sie in Ihrer Web-ACL-Konfiguration alles, was Sie testen möchten, in den Zählmodus. Dadurch zeichnet der Testschutz Treffer mit Webanfragen auf, ohne die Art und Weise zu ändern, wie die Anfragen behandelt werden. Sie können die Treffer in Ihren Metriken, Protokollen und Stichprobenanfragen sehen, um die Übereinstimmungskriterien zu überprüfen und zu verstehen, welche Auswirkungen dies auf Ihren Web-Traffic haben könnte. Regeln, die übereinstimmenden Anfragen Labels hinzufügen, fügen unabhängig von der Regelaktion Labels hinzu.

- In der Web-ACL definierte Regel — Bearbeiten Sie die Regeln in der Web-ACL und legen Sie ihre Aktionen auf festCount.

- Regelgruppe — Bearbeiten Sie in Ihrer Web-ACL-Konfiguration die Regelaussage für die Regelgruppe und öffnen Sie im Bereich Regeln die Dropdownliste Alle Regelaktionen außer Kraft setzen und wählen Sie aus Count. Wenn Sie die Web-ACL in JSON verwalten, fügen Sie die Regeln zu den `RuleActionOverrides` Einstellungen in der Regelgruppen-Referenzanweisung hinzu, wobei der Wert auf `ActionToUse Count` gesetzt ist. Die folgende Beispielliste zeigt Überschreibungen für zwei Regeln in der Regelgruppe „AWSManagedRulesAnonymousIpList AWS Verwaltete Regeln“.

```
"ManagedRuleGroupStatement": {
  "VendorName": "AWS",
  "Name": "AWSManagedRulesAnonymousIpList",
  "RuleActionOverrides": [
    {
      "ActionToUse": {
        "Count": {}
      },
      "Name": "AnonymousIpList"
    },
    {
      "ActionToUse": {
        "Count": {}
      },
      "Name": "HostingProviderIpList"
    }
  ],
  "ExcludedRules": []
},
```

Weitere Informationen über das Außerkraftsetzen von Regelaktionen finden Sie unter [Regelaktionen in einer Regelgruppe überschreiben](#)

Ändern Sie für Ihre eigene Regelgruppe nicht die Regelaktionen in der Regelgruppe selbst. Regelgruppenregeln mit Count Aktion generieren nicht die Metriken oder anderen Artefakte, die Sie für Ihre Tests benötigen. Darüber hinaus wirkt sich die Änderung einer Regelgruppe auf alle Web-ACLs aus, die sie verwenden, während sich die Änderungen in der Web-ACL-Konfiguration nur auf die einzelne Web-ACL auswirken.

- Web-ACL — Wenn Sie eine neue Web-ACL testen, legen Sie als Standardaktion für die Web-ACL fest, dass Anfragen zugelassen werden. Auf diese Weise können Sie die Web-ACL ausprobieren, ohne den Datenverkehr in irgendeiner Weise zu beeinträchtigen.

Im Allgemeinen generiert der Zählmodus mehr Treffer als der Produktionsmodus. Das liegt daran, dass eine Regel, die Anfragen zählt, die Auswertung der Anfrage durch die Web-ACL nicht unterbricht, sodass Regeln, die später in der Web-ACL ausgeführt werden, möglicherweise auch der Anfrage entsprechen. Wenn Sie Ihre Regelaktionen an ihre Produktionseinstellungen anpassen, beenden Regeln, die Anfragen zulassen oder blockieren, die Auswertung der Anfragen, denen sie entsprechen. Das hat zur Folge, dass übereinstimmende Anfragen in der Regel anhand weniger Regeln in der Web-ACL geprüft werden. Weitere Informationen zu den Auswirkungen von Regelaktionen auf die Gesamtbewertung einer Webanfrage finden Sie unter [Regelaktion](#).

Mit diesen Einstellungen wirken sich Ihre neuen Schutzmaßnahmen nicht auf den Web-Traffic aus, sondern generieren Übereinstimmungsinformationen in Metriken, Web-ACL-Protokollen und Anforderungsbeispielen.

3. Zuordnen der Web-ACL zu einer Ressource

Wenn die Web-ACL der Ressource noch nicht zugeordnet ist, ordnen Sie sie zu.

Siehe [Zuordnen oder Aufheben der Zuordnung einer Web-ACL zu einer Ressource AWS](#).

Sie sind jetzt bereit, Ihre Web-ACL zu überwachen und zu optimieren.

Überwachung und Tuning

In diesem Abschnitt wird beschrieben, wie Sie Ihre AWS WAF Schutzmaßnahmen überwachen und optimieren können.

Note

Um den Anleitungen in diesem Abschnitt folgen zu können, müssen Sie allgemein wissen, wie AWS WAF Schutzmaßnahmen wie Web-ACLs, Regeln und Regelgruppen erstellt und verwaltet werden. Diese Informationen wurden in früheren Abschnitten dieses Handbuchs behandelt.

Überwachen Sie den Webverkehr und Regelübereinstimmungen, um das Verhalten der Web-ACL zu überprüfen. Wenn Sie Probleme feststellen, passen Sie Ihre Regeln an, um sie zu korrigieren, und überwachen Sie sie anschließend, um die Anpassungen zu überprüfen.

Wiederholen Sie das folgende Verfahren, bis die Web-ACL Ihren Web-Traffic so verwaltet, wie Sie es benötigen.

Zur Überwachung und Feinabstimmung

1. Überwachen Sie den Datenverkehr und die Regelübereinstimmungen

Stellen Sie sicher, dass der Datenverkehr fließt und dass Ihre Testregeln passende Anfragen finden.

Suchen Sie nach den folgenden Informationen für die Schutzmaßnahmen, die Sie testen:

- **Protokolle** — Greifen Sie auf Informationen zu den Regeln zu, die einer Webanfrage entsprechen:
 - **Ihre Regeln** — Regeln in der Web-ACL, die Count aktiv sind, sind unter `activeNonTerminatingMatchingRules`. Regeln mit Allow oder Block werden als `activeTerminatingRule`. Regeln mit CAPTCHA oder Challenge können entweder beendend oder nicht beendend sein und werden daher je nach Ergebnis des Regelabgleichs in einer der beiden Kategorien aufgeführt.
 - **Regelgruppen** — Regelgruppen werden im `ruleGroupId` Feld identifiziert, wobei ihre Regelübereinstimmungen genauso kategorisiert werden wie bei eigenständigen Regeln.
 - **Labels** — Labels, die Regeln auf die Anfrage angewendet haben, werden in dem `labels` Feld aufgeführt.

Weitere Informationen finden Sie unter [Protokollfelder](#).

- **CloudWatch Amazon-Metriken** — Sie können auf die folgenden Metriken für die Bewertung Ihrer Web-ACL-Anfrage zugreifen.
 - **Ihre Regeln** — Metriken sind nach der Regelaktion gruppiert. Wenn Sie beispielsweise eine Regel im Count Modus testen, werden ihre Treffer als Count Metriken für die Web-ACL aufgeführt.
 - **Ihre Regelgruppen** — Die Metriken für Ihre Regelgruppen sind unter den Regelgruppen-Metriken aufgeführt.
 - **Regelgruppen, die einem anderen Konto gehören** — Regelgruppen-Metriken sind in der Regel nur für den Eigentümer der Regelgruppe sichtbar. Wenn Sie jedoch die Regelaktion für eine Regel überschreiben, werden die Metriken für diese Regel unter Ihren Web-ACL-Metriken aufgeführt. Darüber hinaus werden Labels, die von einer beliebigen Regelgruppe hinzugefügt wurden, in Ihren Web-ACL-Metriken aufgeführt

Regelgruppen in dieser Kategorie sind [AWS Verwaltete Regeln für AWS WAF](#), [AWS Marketplace verwaltete Regelgruppen](#) [Regelgruppen, die von anderen Services bereitgestellt werden](#), und Regelgruppen, die von einem anderen Konto mit Ihnen geteilt wurden.

- Labels — Labels, die während der Evaluierung zu einer Webanfrage hinzugefügt wurden, werden in den Web-ACL-Label-Metriken aufgeführt. Sie können auf die Metriken für alle Labels zugreifen, unabhängig davon, ob sie durch Ihre Regeln und Regelgruppen oder durch Regeln in einer Regelgruppe hinzugefügt wurden, die einem anderen Konto gehört.

Weitere Informationen finden Sie unter [Metriken für Ihre Web-ACL anzeigen](#).

- Dashboards zur Übersicht über den Web-ACL-Traffic — Sie können auf Zusammenfassungen des Web-Traffics zugreifen, den eine Web-ACL ausgewertet hat. Rufen Sie dazu in der AWS WAF Konsole die Seite der Web-ACL auf und öffnen Sie dort die Registerkarte Traffic-Übersicht.

Die Traffic-Übersichts-Dashboards bieten fast in Echtzeit Zusammenfassungen der CloudWatch Amazon-Metriken, die bei der Auswertung des Web-Traffics Ihrer Anwendung AWS WAF erfasst werden.

Weitere Informationen finden Sie unter [Dashboards zur Übersicht über den Web-ACL-Verkehr](#).

- Stichproben von Webanfragen — Greifen Sie auf Informationen zu den Regeln zu, die einer Stichprobe der Webanfragen entsprechen. Die Beispielinformationen identifizieren übereinstimmende Regeln anhand des Metriknamens für die Regel in der Web-ACL. Bei Regelgruppen identifiziert die Metrik die Referenzanweisung für die Regelgruppe. Für Regeln innerhalb von Regelgruppen listet das Beispiel den entsprechenden Regelnamen in `ruleWithinRuleGroup`.

Weitere Informationen finden Sie unter [Anzeigen einer Stichprobe von Webanforderungen](#).

2. Konfigurieren Sie Abhilfemaßnahmen, um Fehlalarme zu beheben

Wenn Sie feststellen, dass eine Regel Fehlalarme generiert, indem sie Webanfragen abgleicht, obwohl dies nicht der Fall sein sollte, können Ihnen die folgenden Optionen dabei helfen, Ihren Web-ACL-Schutz so zu optimieren, dass dieser Fehler behoben wird.

Korrektur der Kriterien für die Überprüfung von Regeln

Für Ihre eigenen Regeln müssen Sie oft nur die Einstellungen anpassen, die Sie zur Überprüfung von Webanfragen verwenden. Beispiele hierfür sind das Ändern der Spezifikationen in einem

Regex-Mustersatz, das Anpassen der Texttransformationen, die Sie vor der Überprüfung auf eine Anforderungskomponente anwenden, oder die Umstellung auf die Verwendung einer weitergeleiteten IP-Adresse. Die Anleitungen für den Regeltyp, der Probleme verursacht, finden Sie unter [Grundlagen der Regelerklärung](#)

Korrigieren komplexerer Probleme

Bei Prüfkriterien, die Sie nicht kontrollieren können, und bei einigen komplexen Regeln müssen Sie möglicherweise weitere Änderungen vornehmen, z. B. Regeln hinzufügen, die Anfragen explizit zulassen oder blockieren oder die Anfragen anhand der problematischen Regel von der Bewertung ausschließen. Für verwaltete Regelgruppen ist diese Art von Schadensbegrenzung am häufigsten erforderlich, aber auch für andere Regeln ist dies möglich. Beispiele hierfür sind die ratenbasierte Regelanweisung und die SQL-Injection-Angriffsregelanweisung.

Was Sie tun, um Fehlalarme zu vermeiden, hängt von Ihrem Anwendungsfall ab. Die folgenden Ansätze sind gebräuchlich:

- Schadensbegrenzungsregel hinzufügen — Fügen Sie eine Regel hinzu, die vor der neuen Regel ausgeführt wird und Anfragen, die zu Fehlalarmen führen, ausdrücklich zulässt. Informationen zur Reihenfolge der Regelauswertung in einer Web-ACL finden Sie unter [Reihenfolge der Verarbeitung von Regeln und Regelgruppen in einer Web-ACL](#).

Bei diesem Ansatz werden die zulässigen Anfragen an die geschützte Ressource gesendet, sodass sie nie die neue Regel zur Auswertung erreichen. Wenn es sich bei der neuen Regel um eine kostenpflichtige verwaltete Regelgruppe handelt, kann dieser Ansatz auch dazu beitragen, die Kosten für die Nutzung der Regelgruppe einzudämmen.

- Eine logische Regel mit einer Schadensbegrenzungsregel hinzufügen — Verwenden Sie logische Regelanweisungen, um die neue Regel mit einer Regel zu kombinieren, die Fehlalarme ausschließt. Weitere Informationen finden Sie unter [Logische Regelaussagen](#).

Angenommen, Sie fügen eine SQL-Injection-Abgleichsanweisung hinzu, die Falschmeldungen für eine Kategorie von Anfragen generiert. Erstellen Sie eine Regel, die diesen Anforderungen entspricht, und kombinieren Sie die Regeln dann mithilfe logischer Regelanweisungen, sodass Sie nur bei Anfragen eine Übereinstimmung erzielen, die sowohl nicht den Kriterien für falsch positive Ergebnisse als auch den Kriterien für SQL-Injection-Angriffe entsprechen.

- Eine Scopedown-Aussage hinzufügen — Schließen Sie bei ratenbasierten Aussagen und Referenzanweisungen für verwaltete Regelgruppen Anfragen, die zu falsch positiven

Ergebnissen führen, von der Auswertung aus, indem Sie der Hauptanweisung eine Scopedown-Aussage hinzufügen.

Eine Anfrage, die nicht mit der Scopedown-Aussage übereinstimmt, erreicht niemals die regelgruppen- oder ratenbasierte Bewertung. Informationen zu Eingrenzungsanweisungen finden Sie unter [Eingrenzungsanweisungen](#). Ein Beispiel finden Sie unter [IP-Bereich von der Bot-Verwaltung ausschließen](#).

- Eine Regel zum Abgleich von Bezeichnungen hinzufügen — Identifizieren Sie für Regelgruppen, die Labels verwenden, die Bezeichnung, die die problematische Regel auf Anfragen anwendet. Möglicherweise müssen Sie die Regelgruppenregeln zuerst im Zählmodus einrichten, falls Sie das noch nicht getan haben. Fügen Sie eine Regel für die Zuordnung von Bezeichnungen hinzu, die so positioniert ist, dass sie hinter der Regelgruppe ausgeführt wird und mit der Bezeichnung übereinstimmt, die durch die problematische Regel hinzugefügt wurde. In der Regel zur Zuordnung von Bezeichnungen können Sie die Anfragen, die Sie zulassen möchten, von den Anfragen, die Sie blockieren möchten, filtern.

Wenn Sie diesen Ansatz verwenden, behalten Sie nach Abschluss des Tests die problematische Regel in der Regelgruppe im Zählmodus und behalten Sie Ihre benutzerdefinierte Regel für den Labelabgleich bei. Informationen zu Anweisungen für Bezeichnungsabgleiche finden Sie unter [Regelanweisung für Bezeichnungsübereinstimmung](#). Beispiele finden Sie unter [Bestimmten blockierten Bot zulassen](#) und [ATP-Beispiel: Benutzerdefinierte Behandlung fehlender und kompromittierter Anmeldeinformationen](#).

- Ändern Sie die Version einer verwalteten Regelgruppe — Ändern Sie bei versionierten verwalteten Regelgruppen die Version, die Sie verwenden. Sie könnten beispielsweise zur letzten statischen Version zurückkehren, die Sie erfolgreich verwendet haben.

Dies ist normalerweise eine vorübergehende Lösung. Sie können die Version für Ihren Produktionsdatenverkehr ändern, während Sie die neueste Version in Ihrer Test- oder Staging-Umgebung weiter testen oder während Sie auf eine kompatiblere Version des Anbieters warten. Informationen zu Versionen verwalteter Regelgruppen finden Sie unter [Verwaltete Regelgruppen](#).

Wenn Sie überzeugt sind, dass die neuen Regeln den Anforderungen wie gewünscht entsprechen, fahren Sie mit der nächsten Testphase fort und wiederholen Sie dieses Verfahren. Führen Sie die letzte Phase der Tests und Optimierungen in Ihrer Produktionsumgebung durch.

Metriken für Ihre Web-ACL anzeigen

Nachdem Sie eine Web-ACL mit einer oder mehreren AWS Ressourcen verknüpft haben, können Sie die resultierenden Metriken für die Zuordnung in einem CloudWatch Amazon-Diagramm anzeigen.

Informationen zu AWS WAF Metriken finden Sie unter [AWS WAF Metriken und Dimensionen](#).

Informationen zu CloudWatch Metriken finden Sie im [CloudWatch Amazon-Benutzerhandbuch](#).

Sie CloudWatch können für jede Ihrer Regeln in einer Web-ACL und für alle Anfragen, an die eine zugehörige Ressource AWS WAF für eine Web-ACL weiterleitet, Folgendes tun:

- Daten für die vorangegangene Stunde oder die letzten drei Stunden anzeigen.
- Ändern Sie das Intervall zwischen Datenpunkten.
- Ändern Sie die Berechnung, CloudWatch die für die Daten ausgeführt wird, z. B. Maximum, Minimum, Durchschnitt oder Summe.

Note

AWS WAF with CloudFront ist ein globaler Service, und Metriken sind nur verfügbar, wenn Sie die Region USA Ost (Nord-Virginia) in der auswählen AWS Management Console. Wenn Sie eine andere Region wählen, werden keine AWS WAF Metriken in der CloudWatch Konsole angezeigt.

So zeigen Sie Daten für die Regeln in einer Web-ACL an

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Ändern Sie bei Bedarf die Region in die Region, in der sich Ihre AWS Ressourcen befinden. Wählen Sie für CloudFront die Region USA Ost (Nord-Virginia) aus.
3. Wählen Sie im Navigationsbereich unter Metriken die Option Alle Metriken aus und suchen Sie dann auf der Registerkarte Durchsuchen nach AWS : : WAFV2.
4. Aktivieren Sie das Kontrollkästchen für die Web-ACL, für die Sie Daten anzeigen möchten.
5. Ändern Sie die geltenden Einstellungen:

Statistik

Wählen Sie die Berechnung CloudWatch aus, die mit den Daten durchgeführt wird.

Zeitraum

Wählen Sie aus, ob die Daten für die letzte Stunde oder für die letzten drei Stunden angezeigt werden sollen.

Intervall

Wählen Sie das Intervall zwischen den Datenpunkten in der Grafik aus.

Regeln

Wählen Sie die Regeln aus, für die Sie Daten anzeigen möchten.

Note

Wenn Sie den Namen einer Regel ändern und möchten, dass der Metrikname der Regel die Änderung widerspiegelt, müssen Sie auch den Metriknamen aktualisieren. AWS WAF aktualisiert den Metriknamen für eine Regel nicht automatisch, wenn Sie den Regelnamen ändern. Sie können den Metriknamen ändern, wenn Sie die Regel in der Konsole bearbeiten, indem Sie den JSON-Editor für Regeln verwenden. Sie können beide Namen auch über die APIs und in jeder JSON-Liste ändern, mit der Sie Ihre Web-ACL oder Regelgruppe definieren.

Beachten Sie Folgendes:

- Wenn Sie kürzlich eine Web-ACL mit einer AWS Ressource verknüpft haben, müssen Sie möglicherweise einige Minuten warten, bis Daten im Diagramm und die Metrik für die Web-ACL in der Liste der verfügbaren Metriken angezeigt wird.
- Wenn Sie einer Web-ACL mehr als eine Ressource zuordnen, enthalten die CloudWatch Daten Anfragen für alle Ressourcen.
- Sie können den Mauszeiger über einen Datenpunkt bewegen, um weitere Informationen zu erhalten.
- Die Grafik wird nicht automatisch aktualisiert. Wählen Sie zum Aktualisieren der Anzeige das Symbol



Weitere Informationen zu CloudWatch Metriken finden Sie unter [Überwachung mit Amazon CloudWatch](#).

Dashboards zur Übersicht über den Web-ACL-Verkehr

In diesem Abschnitt werden die Dashboards mit der Übersicht über den Web-ACL-Verkehr in der AWS WAF Konsole beschrieben. Nachdem Sie eine Web-ACL mit einer oder mehreren AWS Ressourcen verknüpft und Metriken für die Web-ACL aktiviert haben, können Sie auf Zusammenfassungen des Web-Traffics zugreifen, den die Web-ACL auswertet, indem Sie in der Konsole den Tab Traffic Overview der Web-ACL aufrufen. AWS WAF Die Dashboards enthalten fast in Echtzeit Zusammenfassungen der CloudWatch Amazon-Metriken, die bei der Auswertung des Web-Traffics Ihrer Anwendung AWS WAF erfasst werden.

Note

Wenn Sie in den Dashboards nichts sehen, stellen Sie sicher, dass Sie Metriken für die Web-ACL aktiviert haben.

Die Registerkarte „Traffic-Übersicht“ der Web-ACL enthält Dashboards mit Registerkarten mit den folgenden Informationskategorien:

- Gesamter Verkehr — Alle Webanfragen, die die Web-ACL auswertet.

Der Schwerpunkt des Dashboards liegt auf dem Beenden von Aktionen, aber Sie können die Treffer für Zählregeln an den folgenden Stellen einsehen:

- Bereich mit den 10 wichtigsten Regeln dieses Dashboards. Schalten Sie „Zur Zählung wechseln“ um, um Übereinstimmungen mit der Zählregel anzuzeigen.
- Registerkarte mit Stichproben für Anfragen auf der ACL-Webseite. Diese neue Registerkarte enthält eine grafische Darstellung aller Regelübereinstimmungen. Weitere Informationen finden Sie unter [Anzeigen einer Stichprobe von Webanforderungen](#).
- Bot Control — Webanfragen, die die Web-ACL mithilfe der von Bot Control verwalteten Regelgruppe auswertet.

Wenn Sie diese Regelgruppe nicht in Ihrer Web-ACL verwenden, werden auf dieser Registerkarte die Ergebnisse der Auswertung einer Stichprobe Ihres Webverkehrs anhand der Bot-Control-Regeln angezeigt. Auf diese Weise erhalten Sie eine Vorstellung vom Bot-Traffic, den Ihre Anwendung empfängt, und der Vorgang ist kostenlos.

Diese Regelgruppe ist Teil der intelligenten Optionen zur Abwehr von Bedrohungen, die das Unternehmen AWS WAF anbietet. Weitere Informationen finden Sie unter [AWS WAF Bot-Steuerung](#) und [AWS WAF Regelgruppe „Bot-Kontrolle“](#).

- Verhinderung von Kontoübernahmen — Webanfragen, die von der Web-ACL anhand der verwalteten Regelgruppe AWS WAF Fraud Control Account Takeover Prevention (ATP) ausgewertet werden. Diese Registerkarte ist nur verfügbar, wenn Sie diese Regelgruppe in Ihrer Web-ACL verwenden.

Die ATP-Regelgruppe ist Teil der AWS WAF intelligenten Angebote zur Abwehr von Bedrohungen. Weitere Informationen finden Sie unter [AWS WAF Verhinderung von Kontoübernahmen bei der Betrugsbekämpfung \(ATP\)](#) und [AWS WAF Regelgruppe zur Verhinderung von Kontoübernahmen \(ATP\) zur Betrugsbekämpfung](#).

- Betrugsprävention bei der Kontoerstellung — Internetanfragen, die von der Web-ACL anhand der verwalteten Regelgruppe AWS WAF Fraud Control Account Creation Fraud Prevention (ACFP) ausgewertet werden. Diese Registerkarte ist nur verfügbar, wenn Sie diese Regelgruppe in Ihrer Web-ACL verwenden.

Die ACFP-Regelgruppe ist Teil der Angebote zur AWS WAF intelligenten Abwehr von Bedrohungen. Weitere Informationen finden Sie unter [AWS WAF Einrichtung von Konten bei der Betrugsbekämpfung und Betrugsprävention \(ACFP\)](#) und [AWS WAF Regelgruppe Betrugsprävention \(ACFP\) zur Kontoerstellung bei der Betrugsbekämpfung](#).

Die Dashboards basieren auf den CloudWatch Metriken der Web-ACL, und die Grafiken bieten Zugriff auf die entsprechenden Metriken in. CloudWatch Bei intelligenten Dashboards zur Bedrohungsabwehr, wie Bot Control, handelt es sich bei den verwendeten Metriken hauptsächlich um Label-Metriken.

- Eine Liste der bereitgestellten Metriken finden Sie AWS WAF unter. [AWS WAF Metriken und Dimensionen](#)
- Informationen zu CloudWatch Metriken finden Sie im [CloudWatch Amazon-Benutzerhandbuch](#).

Die Dashboards bieten Zusammenfassungen Ihrer Verkehrsmuster für die von Ihnen ausgewählten Abschlussaktionen und den von Ihnen ausgewählten Zeitraum. Die intelligenten Dashboards zur Bedrohungsabwehr enthalten Anfragen, die von der entsprechenden verwalteten Regelgruppe bewertet wurden, unabhängig davon, ob die verwaltete Regelgruppe selbst die beendende Aktion angewendet hat. Wenn diese Option beispielsweise ausgewählt Block ist, enthält das Dashboard

zur Verhinderung von Kontoübernahmen Informationen zu allen Webanfragen, die sowohl von der von ATP verwalteten Regelgruppe bewertet als auch irgendwann während der Web-ACL-Bewertung blockiert wurden. Die Anfragen können durch die von ATP verwaltete Regelgruppe, durch eine Regel, die nach der Regelgruppe in der Web-ACL ausgeführt wurde, oder durch die Web-ACL-Standardaktion blockiert werden.

Dashboards für eine Web-ACL anzeigen

Gehen Sie wie in diesem Abschnitt beschrieben vor, um auf die Web-ACL-Dashboards zuzugreifen und die Datenfilterkriterien festzulegen. Wenn Sie kürzlich eine Web-ACL mit einer AWS Ressource verknüpft haben, müssen Sie möglicherweise einige Minuten warten, bis Daten in den Dashboards verfügbar sind.

Die Dashboards enthalten die Anfragen für alle Ressourcen, die Sie der Web-ACL zugeordnet haben.

So zeigen Sie die Dashboards mit der Traffic-Übersicht für eine Web-ACL an

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich Web-ACLs aus und suchen Sie dann nach der Web-ACL, an der Sie interessiert sind.
3. Wählen Sie die Web-ACL aus. Die Konsole führt Sie zur Seite der Web-ACL. Die Registerkarte Verkehrsübersicht ist standardmäßig ausgewählt.
4. Ändern Sie die Datenfiltereinstellungen nach Bedarf.
 - Regelaktionen beenden — Wählen Sie die beendenden Aktionen aus, die in die Dashboards aufgenommen werden sollen. In den Dashboards werden die Metriken für die Webanfragen zusammengefasst, auf die eine der ausgewählten Aktionen bei der Web-ACL-Bewertung angewendet wurde. Wenn Sie alle verfügbaren Aktionen auswählen, enthalten die Dashboards alle bewerteten Webanfragen. Informationen zu den Aktionen finden Sie unter [So werden Regel- und Regelgruppenaktionen in einer Web-ACL behandelt](#).
 - Zeitraum — Wählen Sie das Zeitintervall aus, das in den Dashboards angezeigt werden soll. Sie können wählen, ob ein Zeitrahmen relativ zum aktuellen Zeitpunkt angezeigt werden soll, z. B. die letzten 3 Stunden oder die letzte Woche, und Sie können einen absoluten Zeitraum aus einem Kalender auswählen.
 - Zeitzone — Diese Einstellung gilt, wenn Sie einen absoluten Zeitraum angeben. Sie können die lokale Zeitzone Ihres Browsers oder UTC (Coordinated Universal Time) verwenden.

Überprüfen Sie die Informationen auf den Tabs, die Sie interessieren. Die Datenfilterauswahl gilt für alle Dashboards. In den Grafikfenstern können Sie den Mauszeiger über einen Datenpunkt oder einen Bereich bewegen, um weitere Details anzuzeigen.

CountAktionsregeln

Sie können Informationen zur Anzahl von Action-Matches an einer von zwei Stellen einsehen.

- Suchen Sie auf dieser Registerkarte „Verkehrsübersicht“ im Dashboard „Gesamter Traffic“ nach dem Bereich „Die 10 wichtigsten Regeln“ und aktivieren Sie die Option „Zur Zählung wechseln“. Wenn dieser Schalter aktiviert ist, wird im Bereich die Anzahl der Übereinstimmungen mit den Regeln angezeigt, anstatt dass die Regelübereinstimmungen beendet werden.
- Auf der Registerkarte Stichprobenanfragen der Web-ACL wird ein Diagramm aller Regelübereinstimmungen und Aktionen für den Zeitraum angezeigt, den Sie auf der Registerkarte Verkehrsübersicht festgelegt haben. Weitere Informationen zum Tab Stichprobenanfragen finden Sie unter [Anzeigen einer Stichprobe von Webanforderungen](#)

CloudWatch Amazon-Metriken

In den Diagrammbereichen des Dashboards können Sie auf die CloudWatch Metriken für die grafisch dargestellten Daten zugreifen. Wählen Sie die Option oben im Grafikfenster oder aus dem Drop-down-Menü (vertikale Ellipse) innerhalb des Bereichs.

Aktualisierung der Dashboards

Die Dashboards werden nicht automatisch aktualisiert. Um die Anzeige zu aktualisieren, wählen Sie das



Aktualisierungssymbol.

Beispiele für die Traffic-Übersichts-Dashboards für Web-ACLs

Dieser Abschnitt zeigt Beispielbildschirme der Traffic-Übersichts-Dashboards für Web-ACLs.

Note

Wenn Sie Ihre Anwendungsressourcen bereits AWS WAF zum Schutz verwenden, können Sie die Dashboards für jede Ihrer Web-ACLs auf der entsprechenden Seite in der Konsole

einsehen. AWS WAF Weitere Informationen finden Sie unter [Dashboards für eine Web-ACL anzeigen](#).

Beispielbildschirm: Datenfilter und Anzahl der Aktionen im Dashboard „Gesamter Traffic“

Der folgende Screenshot zeigt die Verkehrsübersicht für eine Web-ACL, bei der die Registerkarte Gesamter Verkehr ausgewählt ist. Die Datenfilter sind auf die Standardwerte eingestellt: alle beendeten Aktionen der letzten drei Stunden.

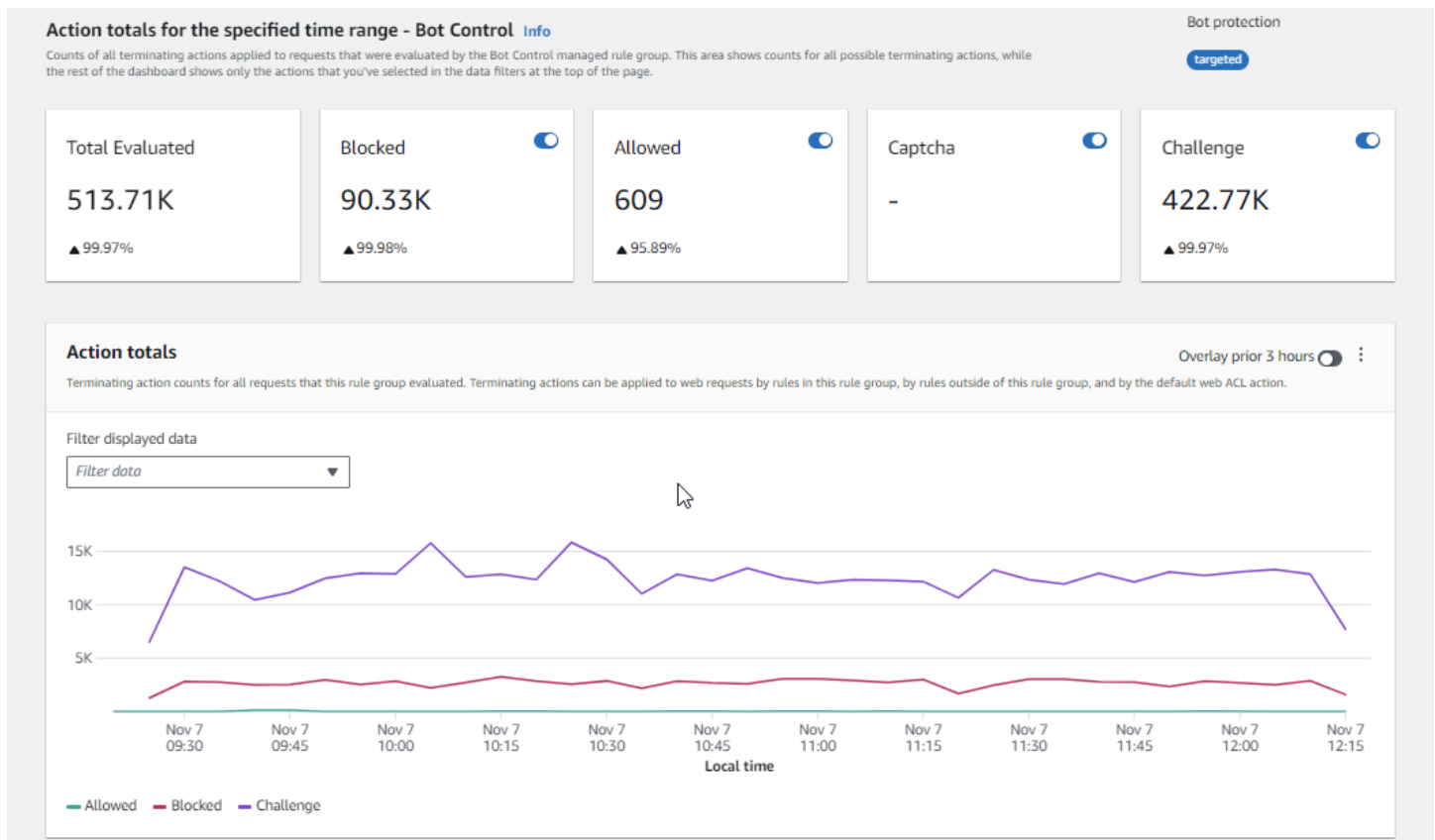
Im Dashboard für den gesamten Verkehr befinden sich die Gesamtwerte der Aktionen für die verschiedenen beendenden Aktionen. In jedem Bereich ist die Anzahl der Anfragen aufgeführt und es wird ein Pfeil nach oben/unten angezeigt, der die Änderung seit den letzten drei Stunden anzeigt.

The screenshot shows the AWS WAF console interface for a Web ACL. The left sidebar contains navigation options for WAF & Shield, AWS WAF, and AWS Shield. The main content area is titled 'DefaultDashboardWebACL' and includes a 'Download web ACL as JSON' button. The 'Traffic overview' tab is active, showing a feedback message and 'Data filters' for 'Terminating rule actions' (set to 'All traffic'), 'Time range' (set to 'Last 3 hours'), and 'Time zone' (set to 'Local time'). Below the filters, there are five action total cards for 'Total', 'Blocked', 'Allowed', 'Captcha', and 'Challenge', each displaying a count and a percentage change from the previous period.

Action	Count	Change (%)
Total	612.91K	▲99.96%
Blocked	180.23K	▲99.96%
Allowed	609	▲95.89%
Captcha	4.58K	▲100%
Challenge	427.49K	▲99.97%

Beispielbildschirm: Anzahl der Aktionen im Bot Control-Dashboard

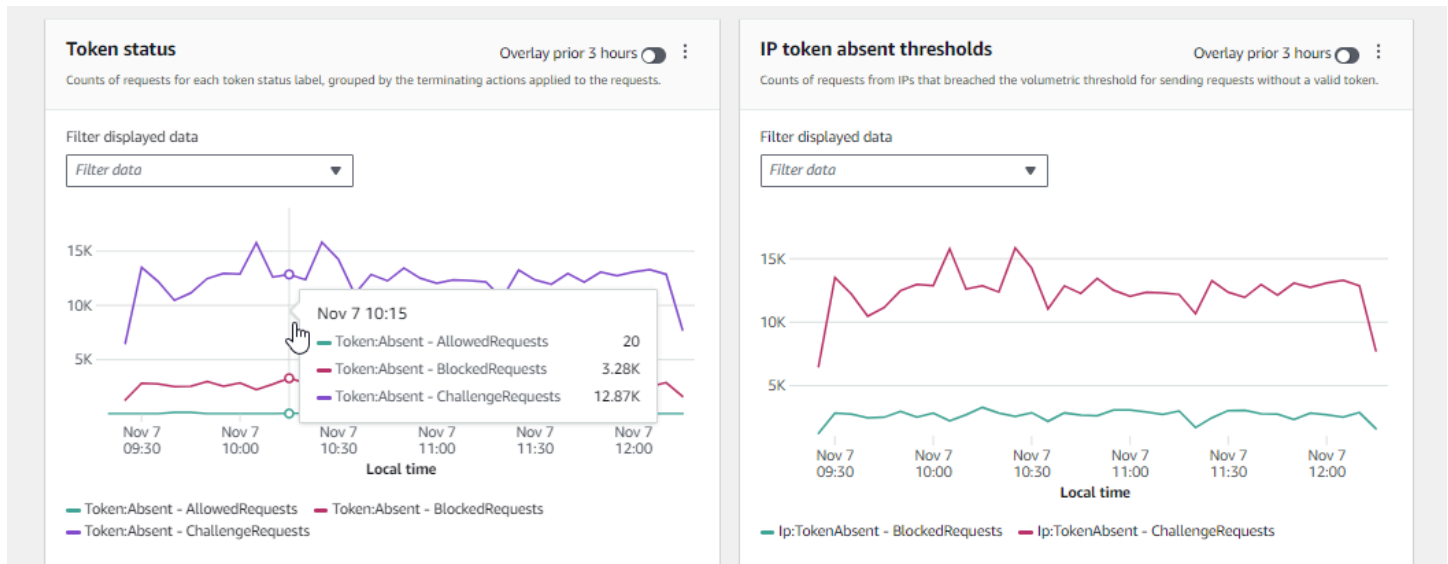
Der folgende Screenshot zeigt die Anzahl der Aktionen für das Bot Control-Dashboard. Hier werden dieselben Summenbereiche für den Zeitraum angezeigt, aber die Anzahl bezieht sich nur auf Anfragen, die von der Bot Control-Regelgruppe ausgewertet wurden. Weiter unten, im Bereich Aktionssummen, können Sie die Anzahl der Aktionen im angegebenen Zeitraum von drei Stunden sehen. Für diesen Zeitraum wurde die CAPTCHA Aktion auf keine der Anfragen angewendet, die von der Regelgruppe ausgewertet wurden.



Beispielbildschirm: Übersichtsdiagramme zum Token-Status im Bot Control-Dashboard

Der folgende Screenshot zeigt zwei der Übersichtsgrafiken, die im Bot Control-Dashboard verfügbar sind. Im Bereich Token-Status werden die Zählungen für die verschiedenen Token-Statusbezeichnungen zusammen mit der Regelaktion angezeigt, die auf die Anfrage angewendet wurde. Im Bereich Schwellenwerte für fehlende IP-Token werden Daten für Anfragen von IPs angezeigt, die zu viele Anfragen ohne Token gesendet haben.

Wenn Sie den Mauszeiger über einen beliebigen Bereich im Diagramm bewegen, werden die verfügbaren Informationen angezeigt. Im Bereich Token-Status in diesem Screenshot bewegt sich die Maus über einem bestimmten Zeitpunkt, ohne sich auf einer Grafikinie zu befinden, sodass in der Konsole die Daten für alle Linien zu diesem Zeitpunkt angezeigt werden.



In diesem Abschnitt werden nur einige der Zusammenfassungen des Datenverkehrs aufgeführt, die in den Web-ACL-Dashboards zur Übersicht über den Datenverkehr bereitgestellt werden. Um die Dashboards für Ihre Web-ACLs zu sehen, öffnen Sie die Seite der Web-ACLs in der Konsole. Informationen dazu, wie Sie dies tun können, finden Sie in der Anleitung unter [Dashboards für eine Web-ACL anzeigen](#)

Anzeigen einer Stichprobe von Webanforderungen


In diesem Abschnitt wird der Tab „Web-ACL Sampled Requests“ in der AWS WAF Konsole beschrieben. Auf dieser Registerkarte können Sie ein Diagramm aller Regelübereinstimmungen für Webanfragen anzeigen, die geprüft AWS WAF wurden. Wenn Sie das Sampling von Anfragen aktiviert haben, können Sie sich außerdem eine tabellarische Ansicht mit einer Stichprobe der Webanfragen ansehen, die geprüft AWS WAF wurden.

Die Stichprobe von Anfragen enthält bis zu 100 Anfragen, die den Kriterien für eine Regel in der Web-ACL entsprachen, und weitere 100 Anfragen für Anfragen, die keiner Regel entsprachen und auf die die Web-ACL-Standardaktion angewendet wurde. Die Anfragen im Beispiel stammen von allen geschützten Ressourcen, die in den letzten drei Stunden Anfragen für Ihre Inhalte erhalten haben.

Wenn eine Webanforderung den Kriterien in einer Regel entspricht und die Aktion für diese Regel die Auswertung der Anfrage nicht beendet, AWS WAF wird die Überprüfung der Webanforderung anhand der nachfolgenden Regeln in der Web-ACL fortgesetzt. Aus diesem Grund kann eine Webanforderung mehrfach erscheinen. Informationen zum Verhalten von Regelaktionen finden Sie unter [Regelaktion](#).

Um das Diagramm mit allen Regeln und die Anzahl der Anfragen in Stichproben anzuzeigen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im Navigationsbereich Web ACLs aus.
3. Wählen Sie den Namen der Web-ACL aus, für die Sie Anforderungen anzeigen möchten. Die Konsole führt Sie zur Beschreibung der Web-ACL, wo Sie sie bearbeiten können.
4. Auf der Registerkarte „Gesampelte Anfragen“ können Sie Folgendes sehen:
 - Diagramm „Alle Regeln“ — Dieses Diagramm zeigt die passenden Regeln und Regelaktionen für alle Evaluierungen von Webanfragen, die im angegebenen Zeitraum durchgeführt wurden.


 Note

Der Zeitraum für dieses Diagramm wird auf der Registerkarte Verkehrsübersicht der Web-ACL im Bereich Datenfilter festgelegt. Weitere Informationen finden Sie unter [Dashboards für eine Web-ACL anzeigen](#).

- Tabelle mit Stichprobenanfragen — In dieser Tabelle werden Stichprobendaten der letzten 3 Stunden angezeigt. Für jeden Eintrag werden in der Tabelle die folgenden Daten angezeigt:

Metrikname

Der CloudWatch Metrikname für die Regel in der Web-ACL, die der Anfrage entspricht. Wenn eine Webanforderung keiner Regel in der Web-ACL entspricht, ist dieser Wert Standard.

 Note

Wenn Sie den Namen einer Regel ändern und möchten, dass der Metrikname der Regel die Änderung widerspiegelt, müssen Sie auch den Metriknamen aktualisieren. AWS WAF aktualisiert den Metriknamen für eine Regel nicht automatisch, wenn Sie den Regelnamen ändern. Sie können den Metriknamen ändern, wenn Sie die Regel in der Konsole bearbeiten, indem Sie den JSON-Editor für Regeln verwenden. Sie können beide Namen auch über die APIs und in jeder JSON-Liste ändern, mit der Sie Ihre Web-ACL oder Regelgruppe definieren.

Quell-IP

Entweder die IP-Adresse, von der die Anforderung stammt, oder – falls das Anzeigeprogramm zum Senden der Anforderung einen HTTP-Proxy oder einen Application Load Balancer verwendet hat – die IP-Adresse des Proxys oder des Application Load Balancer.

URI

Der Teil einer URL, der eine Ressource angibt, z. B. `/images/daily-ad.jpg`.

Regel innerhalb der Regelgruppe

Wenn der Metrikname eine Referenzanweisung für eine Regelgruppe identifiziert, identifiziert dies die Regel innerhalb der Regelgruppe, die der Anforderung entsprach.

Aktion

Zeigt die Aktion für die entsprechende Regel an. Informationen zu den möglichen Regelaktionen finden Sie unter [Regelaktion](#).

Zeit

Die Uhrzeit, zu der die Anfrage von der geschützten Ressource AWS WAF empfangen wurde.

Um zusätzliche Informationen zu den Komponenten einer Webanfrage anzuzeigen, wählen Sie den Namen des URI in der Zeile der Anfrage aus.

Aktivierung Ihres Schutzes in der Produktion

Wenn Sie die letzte Phase der Tests und Optimierungen in Ihrer Produktionsumgebung abgeschlossen haben, aktivieren Sie Ihre Schutzmaßnahmen im Produktionsmodus.

Risiken rund um Produktionsdatenverkehr

Bevor Sie Ihre Web-ACL-Implementierung für den Produktionsdatenverkehr einsetzen, testen und optimieren Sie sie in einer Testumgebung, bis Sie mit den möglichen Auswirkungen auf Ihren Datenverkehr zufrieden sind. Testen und optimieren Sie sie außerdem im

Zählmodus mit Ihrem Produktionsdatenverkehr, bevor Sie Ihre Schutzmaßnahmen für den Produktionsdatenverkehr aktivieren.

Note

Um den Anleitungen in diesem Abschnitt folgen zu können, müssen Sie allgemein wissen, wie AWS WAF Schutzmaßnahmen wie Web-ACLs, Regeln und Regelgruppen erstellt und verwaltet werden. Diese Informationen wurden in früheren Abschnitten dieses Handbuchs behandelt.

Führen Sie diese Schritte zuerst in Ihrer Testumgebung und dann in der Produktion durch.

Aktivieren Sie Ihre AWS WAF Schutzmaßnahmen in der Produktion

1. Wechseln Sie zu Ihren Produktionsschutzmaßnahmen

Aktualisieren Sie Ihre Web-ACL und ändern Sie Ihre Einstellungen für die Produktion.

a. Entfernen Sie alle Testregeln, die Sie nicht benötigen

Wenn Sie Testregeln hinzugefügt haben, die Sie in der Produktion nicht benötigen, entfernen Sie sie. Wenn Sie Regeln für den Labelabgleich verwenden, um die Ergebnisse verwalteter Regelgruppenregeln zu filtern, achten Sie darauf, dass diese unverändert bleiben.

b. Wechseln Sie zu Produktionsaktionen

Ändern Sie die Aktionseinstellungen für Ihre neuen Regeln auf die vorgesehenen Produktionseinstellungen.

- In der Web-ACL definierte Regel — Bearbeiten Sie die Regeln in der Web-ACL und ändern Sie ihre Aktionen von Count zu ihren Produktionsaktionen.
- Regelgruppe — Ändern Sie in Ihrer Web-ACL-Konfiguration der Regelgruppe die Regeln so, dass sie ihre eigenen Aktionen verwenden, oder belassen Sie sie, je nach den Ergebnissen Ihrer Test- und Optimierungsaktivitäten, bei der Count Aktionsüberschreibung. Wenn Sie eine Regel für den Labelabgleich verwenden, um die Ergebnisse einer Regelgruppenregel zu filtern, achten Sie darauf, die Überschreibung für diese Regel beizubehalten.

Um zur Verwendung der Aktion einer Regel zu wechseln, bearbeiten Sie in Ihrer Web-ACL-Konfiguration die Regelanweisung für die Regelgruppe und entfernen Sie die Count Außerkräftsetzung für die Regel. Wenn Sie die Web-ACL in JSON verwalten, entfernen Sie in der Referenzanweisung für die Regelgruppe den Eintrag für die Regel aus der `RuleActionOverrides` Liste.

- Web-ACL — Wenn Sie die Web-ACL-Standardaktion für Ihre Tests geändert haben, stellen Sie sie auf die Produktionseinstellung um.

Mit diesen Einstellungen verwalten Ihre neuen Schutzmaßnahmen den Web-Traffic wie gewünscht.

Wenn Sie Ihre Web-ACL speichern, verwenden die Ressourcen, denen sie zugeordnet ist, Ihre Produktionseinstellungen.

2. Überwachen und Anpassen

Um sicherzustellen, dass Webanfragen wie gewünscht bearbeitet werden, sollten Sie Ihren Datenverkehr genau beobachten, nachdem Sie die neue Funktion aktiviert haben. Sie werden die Messwerte und Protokolle für die Aktionen Ihrer Produktionsregeln überwachen und nicht die Anzahl der Aktionen, auf die Sie bei der Optimierung geachtet haben. Überwachen Sie weiter und passen Sie das Verhalten nach Bedarf an, um es an Änderungen in Ihrem Web-Traffic anzupassen.

Wie AWS WAF funktioniert mit CloudFront Amazon-Funktionen

Wenn Sie eine Web-ACL erstellen, können Sie eine oder mehrere CloudFront Distributionen angeben, die Sie überprüfen AWS WAF möchten. AWS WAF beginnt mit der Prüfung und Verwaltung von Webanfragen für diese Distributionen auf der Grundlage der Kriterien, die Sie in der Web-ACL angeben. CloudFront bietet einige Funktionen, die die AWS WAF Funktionalität erweitern. In diesem Kapitel werden einige Möglichkeiten beschrieben, die Sie konfigurieren können CloudFront , um die Zusammenarbeit CloudFront und AWS WAF Zusammenarbeit zu verbessern.

Themen

- [Verwendung AWS WAF mit CloudFront benutzerdefinierten Fehlerseiten](#)
- [Verwenden Sie AWS WAF with CloudFront für Anwendungen, die auf Ihrem eigenen HTTP-Server ausgeführt werden](#)

- [Auswahl der HTTP-Methoden, die CloudFront darauf reagieren](#)

Verwendung AWS WAF mit CloudFront benutzerdefinierten Fehlerseiten

Wenn eine Webanforderung auf der Grundlage der von Ihnen angegebenen Kriterien AWS WAF blockiert wird, wird standardmäßig der HTTP-Statuscode 403 (Forbidden) an CloudFront zurückgegeben und dieser Statuscode wird an den Betrachter zurückgegeben. Dieser zeigt dann eine kurze und kaum formatierte Standardnachricht an, ähnlich wie diese:

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

Sie können dieses Verhalten in Ihren AWS WAF Web-ACL-Regeln überschreiben, indem Sie benutzerdefinierte Antworten definieren. Weitere Informationen zum Anpassen des Antwortverhaltens mithilfe von AWS WAF Regeln finden Sie unter [Benutzerdefinierte Antworten für Block Aktionen](#).

Note

Antworten, die Sie mithilfe von AWS WAF Regeln anpassen, haben Vorrang vor allen Antwortspezifikationen, die Sie auf CloudFront benutzerdefinierten Fehlerseiten definieren.

Wenn Sie lieber eine benutzerdefinierte Fehlermeldung anzeigen und dabei möglicherweise dieselbe Formatierung wie der Rest Ihrer Website verwenden möchten, können Sie so konfigurieren CloudFront, dass ein Objekt (z. B. eine HTML-Datei), das Ihre benutzerdefinierte Fehlermeldung enthält, an den Betrachter zurückgegeben wird.

Note

CloudFront kann nicht zwischen einem HTTP-Statuscode 403, der von Ihrem Ursprung zurückgegeben wird, und einem, der zurückgegeben wird, AWS WAF wenn eine Anfrage blockiert wird, unterscheiden. Das heißt, Sie können keine unterschiedlichen benutzerdefinierten Fehlerseiten basierend auf den verschiedenen Ursachen für den HTTP-Statuscode 403 zurückgeben.

Weitere Informationen zu CloudFront benutzerdefinierten Fehlerseiten finden Sie unter [Generieren benutzerdefinierter Fehlerantworten](#) im Amazon CloudFront Developer Guide.

Verwenden Sie AWS WAF with CloudFront für Anwendungen, die auf Ihrem eigenen HTTP-Server ausgeführt werden

Wenn Sie AWS WAF mit verwenden CloudFront, können Sie Ihre Anwendungen schützen, die auf einem beliebigen HTTP-Webserver ausgeführt werden, unabhängig davon, ob es sich um einen Webserver handelt, der in Amazon Elastic Compute Cloud (Amazon EC2) läuft, oder um einen Webserver, den Sie privat verwalten. Sie können auch so konfigurieren CloudFront , dass HTTPS zwischen CloudFront und Ihrem eigenen Webserver sowie zwischen Zuschauern und erforderlich ist. CloudFront

HTTPS zwischen CloudFront und Ihrem eigenen Webserver erforderlich

Um HTTPS zwischen CloudFront und Ihrem eigenen Webserver zu verlangen, können Sie die CloudFront benutzerdefinierte Origin-Funktion verwenden und die Origin-Protokollrichtlinie und die Origin-Domainnamen-Einstellungen für bestimmte Ursprünge konfigurieren. In Ihrer CloudFront Konfiguration können Sie den DNS-Namen des Servers zusammen mit dem Port und dem Protokoll angeben, das Sie beim Abrufen von Objekten von Ihrem Ursprung verwenden CloudFront möchten. Außerdem sollten Sie sicherstellen, dass das SSL/TLS-Zertifikat auf Ihrem benutzerdefinierten Ursprungs-Server mit dem von Ihnen konfigurierten Ursprungsdomännennamen übereinstimmt. Wenn Sie Ihren eigenen HTTP-Webserver außerhalb von verwenden AWS, müssen Sie ein Zertifikat verwenden, das von einer vertrauenswürdigen Zertifizierungsstelle (CA) eines Drittanbieters, z. B. Comodo oder Symantec, signiert wurde. DigiCert Weitere Informationen darüber, wie HTTPS für die Kommunikation zwischen Ihrem eigenen Webserver CloudFront und Ihrem eigenen Webserver [erforderlich ist, finden Sie im Amazon CloudFront Developer Guide unter HTTPS für die Kommunikation zwischen CloudFront und Ihrem benutzerdefinierten Ursprung](#) erforderlich.

HTTPS zwischen einem Betrachter erforderlich und CloudFront

Um HTTPS zwischen Zuschauern und vorzuschreiben CloudFront, können Sie die Viewer-Protokollrichtlinie für ein oder mehrere Cache-Verhaltensweisen in Ihrer CloudFront Distribution ändern. Weitere Informationen zur Verwendung von HTTPS zwischen Zuschauern und CloudFront finden Sie im Thema [HTTPS für die Kommunikation zwischen Zuschauern erforderlich und CloudFront](#) im Amazon CloudFront Developer Guide. Sie können auch Ihr eigenes SSL-Zertifikat mitbringen, damit Zuschauer über HTTPS eine Verbindung zu Ihrer CloudFront Distribution herstellen können, indem Sie Ihren eigenen Domainnamen verwenden, zum Beispiel `https://www.mysite.com`. Weitere Informationen finden Sie im Thema [Konfiguration alternativer Domainnamen und HTTPS](#) im Amazon CloudFront Developer Guide.

Auswahl der HTTP-Methoden, die CloudFront darauf reagieren

Wenn Sie eine CloudFront Amazon-Webdistribution erstellen, wählen Sie die HTTP-Methoden aus, die Sie verarbeiten und CloudFront an Ihren Ursprung weiterleiten möchten. Sie können aus den folgenden Optionen auswählen:


- **GET, HEAD** — Sie können sie CloudFront nur verwenden, um Objekte von Ihrem Ursprung abzurufen oder um Objekt-Header abzurufen.
- **GET, HEAD, OPTIONS** — Sie können CloudFront nur verwenden, um Objekte von Ihrem Ursprung abzurufen, Objekt-Header abzurufen oder eine Liste der Optionen abzurufen, die Ihr Original-Server unterstützt.
- **GET, HEAD, OPTIONS, PUTPOST, PATCH, DELETE** — Sie können CloudFront Objekte abrufen, hinzufügen, aktualisieren und löschen sowie Objekt-Header abrufen. Darüber hinaus können Sie andere POST-Vorgänge wie das Senden von Daten aus einem Webformular ausführen.

Sie können auch AWS WAF Byte-Match-Regelanweisungen verwenden, um Anfragen, die auf der HTTP-Methode basieren, zuzulassen oder zu blockieren, wie unter beschrieben [Zeichenfolgen-Übereinstimmungsanweisung](#). Wenn Sie eine Kombination von Methoden verwenden möchten, die CloudFront Unterstützung bieten, z. B. GET und HEAD, müssen Sie die Konfiguration nicht so konfigurieren AWS WAF , dass Anfragen blockiert werden, die die anderen Methoden verwenden. Wenn Sie eine Kombination von Methoden zulassen möchten, die CloudFront nicht unterstützt werden, z. B. GET, und HEADPOST, können Sie so konfigurieren CloudFront , dass auf alle Methoden reagiert wird, und dann Anfragen blockieren, die andere Methoden verwenden. AWS WAF

Weitere Informationen zur Auswahl der Methoden, CloudFront auf die reagiert, finden Sie unter [Zulässige HTTP-Methoden](#) im Thema [Werte, die Sie beim Erstellen oder Aktualisieren einer Web-Distribution angeben](#) im Amazon CloudFront Developer Guide.

Sicherheit bei der Nutzung des AWS WAF Dienstes

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

 Note

Dieser Abschnitt enthält AWS Standardsicherheitsrichtlinien für Ihre Nutzung des AWS WAF Dienstes und seiner AWS Ressourcen, wie AWS WAF Web-ACLs und Regelgruppen. Informationen zum Schutz Ihrer AWS Ressourcen mithilfe von Cookies AWS WAF finden Sie im Rest des AWS WAF Handbuchs.

Sicherheit ist eine gemeinsame Verantwortung zwischen Ihnen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Die Wirksamkeit unserer Sicherheitsfunktionen wird regelmäßig von externen Prüfern im Rahmen des [AWS -Compliance-Programms getestet und überprüft](#). Weitere Informationen zu den Compliance-Programmen, die für gelten AWS WAF, finden Sie unter [AWS Services in Umfang nach Compliance-Programmen](#).
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. In Ihre Verantwortung fallen außerdem weitere Faktoren, wie z. B. die Vertraulichkeit der Daten, die Anforderungen Ihrer Organisation sowie geltende Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung anwenden können AWS WAF. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen AWS WAF , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer AWS WAF Ressourcen unterstützen.

Themen

- [Datenschutz in AWS WAF](#)
- [Identitäts- und Zugriffsmanagement für AWS WAF](#)
- [Einloggen und Überwachen AWS WAF](#)
- [Konformitätsvalidierung für AWS WAF](#)
- [Resilienz in AWS WAF](#)
- [Sicherheit der Infrastruktur in AWS WAF](#)

Datenschutz in AWS WAF

Das [Modell der AWS gemeinsamen Verantwortung](#) und geteilter Verantwortung gilt für den Datenschutz in AWS WAF. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter [Häufig gestellte Fragen zum Datenschutz](#). Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag [AWS -Modell der geteilten Verantwortung und in der DSGVO](#) im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-2](#).

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole, der API AWS WAF oder den SDKs arbeiten oder diese anderweitig AWS-Services verwenden. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine

Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

AWS WAF Entitäten — wie Web-ACLs, Regelgruppen und IP-Sets — werden im Ruhezustand verschlüsselt, außer in bestimmten Regionen, in denen Verschlüsselung nicht verfügbar ist, darunter China (Peking) und China (Ningxia). Eindeutige Verschlüsselungsschlüssel werden für jede Region verwendet.

Ressourcen werden gelöscht AWS WAF

Sie können die Ressourcen löschen, die Sie in AWS WAF erstellen. In den folgenden Abschnitten finden Sie Anleitungen für die verschiedenen Ressourcentypen.

- [Löschen einer Web-ACL](#)
- [Löschen einer Regelgruppe](#)
- [Löschen eines IP-Sets](#)
- [Löschen eines Regex-Mustersatzes](#)

Identitäts- und Zugriffsmanagement für AWS WAF

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. AWS WAF IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [Wie AWS WAF funktioniert mit IAM](#)
- [Beispiele für identitätsbasierte Richtlinien für AWS WAF](#)
- [AWS verwaltete Richtlinien für AWS WAF](#)
- [Fehlerbehebung bei AWS WAF Identität und Zugriff](#)

- [Verwenden von serviceverknüpften Rollen für AWS WAF](#)

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie tätig sind. AWS WAF

Dienstbenutzer — Wenn Sie den AWS WAF Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr AWS WAF Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Unter [Fehlerbehebung bei AWS WAF Identität und Zugriff](#) finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Funktion in AWS WAF haben.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die AWS WAF Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf AWS WAF. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS WAF Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM nutzen kann AWS WAF, finden Sie unter [Wie AWS WAF funktioniert mit IAM](#).

IAM-Administrator: Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf AWS WAF verfassen können. Beispiele für AWS WAF identitätsbasierte Richtlinien, die Sie in IAM verwenden können, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS WAF](#)

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen

Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter [So melden Sie sich bei Ihrem an AWS-Konto](#) im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu [signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen](#) signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter [Multi-Faktor-Authentifizierung](#) im AWS IAM Identity Center - Benutzerhandbuch und [Verwenden der Multi-Faktor-Authentifizierung \(MFA\) in AWS](#) im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine

Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter [Was ist IAM Identity Center?](#) im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Eine [IAM-Gruppe](#) ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter [Erstellen eines IAM-Benutzers \(anstatt einer Rolle\)](#) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen [wechseln](#). Sie können eine Rolle übernehmen, indem Sie eine AWS

CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter [Verwenden von IAM-Rollen](#) im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- **Verbundbenutzerzugriff:** Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter [Erstellen von Rollen für externe Identitätsanbieter](#) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze](#) im AWS IAM Identity Center -Benutzerhandbuch.
- **Temporäre IAM-Benutzerberechtigungen:** Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- **Kontoübergreifender Zugriff** – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien](#) im IAM-Benutzerhandbuch.
- **Serviceübergreifender Zugriff** — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
- **Forward Access Sessions (FAS)** — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen

mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

- **Servicerolle:** Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.
- **Dienstbezogene Rolle** — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer Service-Verknüpfung verbunden ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-Verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- **Auf Amazon EC2 ausgeführte Anwendungen** — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter [Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden](#) im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter [Erstellen einer IAM-Rolle \(anstatt eines Benutzers\)](#) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter [Auswahl zwischen verwalteten und eingebundenen Richtlinien](#) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen

in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen zu ACLs finden Sie unter [Zugriffssteuerungsliste \(ACL\) – Übersicht](#) (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- **Berechtigungsgrenzen:** Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im IAM-Benutzerhandbuch.
- **Service Control Policies (SCPs)** — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten, die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos

Weitere Informationen zu Organisationen und SCPs finden Sie unter [Funktionsweise von SCPs](#) im AWS Organizations -Benutzerhandbuch.

- **Sitzungsrichtlinien:** Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

Wie AWS WAF funktioniert mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf verwenden, sollten Sie sich darüber informieren AWS WAF, mit welchen IAM-Funktionen Sie arbeiten können. AWS WAF

IAM-Funktionen, die Sie mit verwenden können AWS WAF

IAM-Feature	AWS WAF Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Ja
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (servicespezifisch)	Ja
ACLs	Nein

IAM-Feature	AWS WAF Unterstützung
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie AWS WAF und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im [IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren](#).

Identitätsbasierte Richtlinien für AWS WAF

Unterstützt Richtlinien auf Identitätsbasis.	Ja
--	----

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

Beispiele für AWS WAF identitätsbasierte Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS WAF](#)

Ressourcenbasierte Richtlinien finden Sie in AWS WAF

Unterstützt ressourcenbasierte Richtlinien	Ja
--	----

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentsität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter [Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden](#) im IAM-Benutzerhandbuch.

AWS WAF verwendet ressourcenbasierte Richtlinien, um die gemeinsame Nutzung von Regelgruppen zwischen Konten zu unterstützen. Sie teilen eine Regelgruppe, die Sie besitzen, mit einem anderen AWS Konto, indem Sie die ressourcenbasierten Richtlinieneinstellungen für den AWS WAF API-Aufruf `PutPermissionPolicy` oder einen entsprechenden CLI- oder SDK-Aufruf bereitstellen. Weitere Informationen, einschließlich Beispielen und Links zur Dokumentation für die anderen verfügbaren Sprachen, finden Sie [PutPermissionPolicy](#) in der AWS WAF API-Referenz. Diese Funktionalität ist nicht auf andere Weise verfügbar, z. B. über die Konsole oder AWS CloudFormation.

Politische Maßnahmen für AWS WAF

Unterstützt Richtlinienaktionen	Ja
---------------------------------	----

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der AWS WAF Aktionen und Berechtigungen für die einzelnen Aktionen finden Sie unter [Von AWS WAF V2 definierte Aktionen](#) in der Serviceautorisierungsreferenz.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS WAF verwendet:

```
wafv2
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [  
  "wafv2:action1",  
  "wafv2:action2"  
]
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Um beispielsweise alle Aktionen anzugeben, die mit `beginnen` AWS WAF `List`, schließen Sie die folgende Aktion ein:

```
"Action": "wafv2:List*"
```

Beispiele für AWS WAF identitätsbasierte Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS WAF](#)

Aktionen, für die zusätzliche Berechtigungseinstellungen erforderlich sind

Für einige Aktionen sind Berechtigungen erforderlich, die im Abschnitt [Von AWS WAF V2 definierte Aktionen](#) in der Serviceautorisierungsreferenz nicht vollständig beschrieben werden können. Dieser Abschnitt enthält zusätzliche Informationen zu Berechtigungen.

Themen

- [Berechtigungen für AssociateWebACL](#)
- [Berechtigungen für DisassociateWebACL](#)
- [Berechtigungen für GetWebACLForResource](#)
- [Berechtigungen für ListResourcesForWebACL](#)

Berechtigungen für **AssociateWebACL**

In diesem Abschnitt sind die Berechtigungen aufgeführt, die erforderlich sind, um einer Ressource mithilfe der AWS WAF Aktion eine Web-ACL zuzuordnen `AssociateWebACL`.

Verwenden Sie für CloudFront Amazon-Verteilungen anstelle dieser Aktion die CloudFront Aktion `UpdateDistribution`. Weitere Informationen finden Sie [UpdateDistribution](#) in der Amazon CloudFront API-Referenz.

Amazon API Gateway API-Gateway-REST-API

Erfordert die Erlaubnis, API Gateway für `SetWebACL` den REST-API-Ressourcentyp aufzurufen und eine Web-ACL AWS WAF `AssociateWebACL` aufzurufen.

```
{
  "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

Erfordert die Berechtigung, `elasticloadbalancing:SetWebACL` Aktionen für den Application Load Balancer Balancer-Ressourcentyp aufzurufen und eine Web-ACL AWS WAF `AssociateWebACL` aufzurufen.

```

{
  "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 GraphQL-API

Erfordert die Berechtigung `AWS AppSync SetWebACL` zum Aufrufen des GraphQL-API-Ressourcentyps und `AWS WAF AssociateWebACL` zum Aufrufen einer Web-ACL.

```

{
  "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/*"
  ]
}

```

Amazon-Cognito-Benutzerpool

Erfordert die Erlaubnis, die Amazon Cognito AssociateWebACL Cognito-Aktion für den Ressourcentyp des Benutzerpools aufzurufen und eine Web-ACL AWS WAF AssociateWebACL aufzurufen.

```

{
  "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 Dienst

Erfordert die Erlaubnis, die `AssociateWebACL Runner`-Aktion für den App Runner-Dienstressourcentyp aufzurufen und eine Web-ACL `AWS WAF AssociateWebACL` aufzurufen.

```
{
  "Sid": "AssociateWebACL1",
  "Effect": "Allow",
  "Action": [
    "wafv2:AssociateWebACL"
  ],
  "Resource": [
    "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
  ]
},
{
  "Sid": "AssociateWebACL2",
  "Effect": "Allow",
  "Action": [
    "apprunner:AssociateWebAc1"
  ],
  "Resource": [
    "arn:aws:apprunner:*:account-id:service/*/*"
  ]
}
```

AWS Verifizierte Access-Instanz

Erfordert die Erlaubnis, die `ec2:AssociateVerifiedAccessInstanceWebAc1` Aktion für den Ressourcentyp „Verified Access“ aufzurufen und eine Web-ACL `AWS WAF AssociateWebACL` aufzurufen.

```
{
  "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/*"
    ]
}

```

Berechtigungen für **DisassociateWebACL**

In diesem Abschnitt sind die Berechtigungen aufgeführt, die erforderlich sind, um eine Web-ACL mithilfe der AWS WAF Aktion `DisassociateWebACL` von einer Ressource zu trennen.

Verwenden Sie für CloudFront Amazon-Verteilungen anstelle dieser Aktion die CloudFront Aktion `UpdateDistribution` mit einer leeren Web-ACL-ID. Weitere Informationen finden Sie [UpdateDistribution](#) in der Amazon CloudFront API-Referenz.

Amazon API Gateway API-Gateway-REST-API

Erfordert die Erlaubnis, API Gateway für `SetWebACL` den REST-API-Ressourcentyp aufzurufen. Erfordert keine Anruferlaubnis AWS WAF `DisassociateWebACL`.

```

{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}

```

Application Load Balancer

Erfordert die Erlaubnis, die `elasticloadbalancing:SetWebACL` Aktion für den Application Load Balancer Balancer-Ressourcentyp aufzurufen. Erfordert keine AWS WAF `DisassociateWebACL` Anruferlaubnis.

```

{

```

```

    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:SetWebACL"
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}

```

AWS AppSync GraphQL-API

Erfordert die Erlaubnis, AWS AppSync SetWebACL den GraphQL-API-Ressourcentyp aufzurufen.

Erfordert keine Erlaubnis zum Aufrufen. AWS WAF DisassociateWebACL

```

{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}

```

Amazon-Cognito-Benutzerpool

Erfordert die Erlaubnis, die Amazon Cognito DisassociateWebACL Cognito-Aktion für den

Ressourcentyp des Benutzerpools aufzurufen und aufzurufen 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 Dienst

Erfordert die Erlaubnis, die App DisassociateWebACL Runner-Aktion für den App Runner-Dienstressourcentyp aufzurufen und aufzurufen 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 Verifizierte Access-Instanz

Erfordert die Erlaubnis, die ec2:DisassociateVerifiedAccessInstanceWebAcl Aktion für den Ressourcentyp „Verified Access“ aufzurufen und aufzurufen 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/*"
    ]
}

```

Berechtigungen für **GetWebACLForResource**

In diesem Abschnitt sind die Berechtigungen aufgeführt, die erforderlich sind, um mithilfe der AWS WAF Aktion die Web-ACL für eine geschützte Ressource abzurufen `GetWebACLForResource`.

Verwenden Sie für CloudFront Amazon-Verteilungen anstelle dieser Aktion die CloudFront Aktion `GetDistributionConfig`. Weitere Informationen finden Sie [GetDistributionConfig](#) in der Amazon CloudFront API-Referenz.

Note

`GetWebACLForResource` benötigt die Erlaubnis zum Aufrufen `GetWebACL`. Wird in diesem Zusammenhang `GetWebACL` nur AWS WAF verwendet, um zu überprüfen, ob Ihr Konto über die erforderliche Berechtigung für den Zugriff auf die `GetWebACLForResource` zurückgesendete Web-ACL verfügt. Wenn Sie aufrufen `GetWebACLForResource`, wird möglicherweise eine Fehlermeldung angezeigt, die darauf hinweist, dass Ihr Konto nicht autorisiert ist, `wafv2:GetWebACL` auf der Ressource zu arbeiten. AWS WAF fügt diese Art von Fehler nicht zum AWS CloudTrail Ereignisverlauf hinzu.

Amazon API Gateway, REST-API, Application Load Balancer und AWS AppSync GraphQL-API

Erfordert die Erlaubnis zum Aufrufen AWS WAF `GetWebACLForResource` und `GetWebACL` für eine Web-ACL.

```

{
  "Sid": "GetWebACLForResource",
  "Effect": "Allow",
  "Action": [
    "wafv2:GetWebACLForResource",
    "wafv2:GetWebACL"
  ],
  "Resource": [
    "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
  ]
}

```

}

Amazon-Cognito-Benutzerpool

Erfordert die Erlaubnis, die Amazon Cognito `GetWebACLForResource` Cognito-Aktion für den Ressourcentyp des Benutzerpools aufzurufen und aufzurufen AWS WAF `GetWebACLForResource`. `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 Dienst

Erfordert die Erlaubnis, die App `DescribeWebACLForService` Runner-Aktion für den App Runner-Dienstressourcentyp aufzurufen und AWS WAF `GetWebACLForResource` und `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 Verifizierte Access-Instanz

Erfordert die Erlaubnis, die `ec2:GetVerifiedAccessInstanceWebAcl` Aktion für den Ressourcentyp „Verified Access“ aufzurufen und AWS WAF `GetWebACLForResource` und `GetWebACL` aufzurufen.

```

{
  "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/*"
  ]
}

```

Berechtigungen für `ListResourcesForWebACL`

In diesem Abschnitt sind die Berechtigungen aufgeführt, die erforderlich sind, um die Liste der geschützten Ressourcen für eine Web-ACL mithilfe der AWS WAF Aktion `ListResourcesForWebACL` abzurufen.

Verwenden Sie für CloudFront Amazon-Verteilungen anstelle dieser Aktion die CloudFront Aktion `ListDistributionsByWebACLId`. Weitere Informationen finden Sie unter [ListDistributionsByWebACLId](#) in der Amazon CloudFront API-Referenz.

Amazon API Gateway, REST-API, Application Load Balancer und AWS AppSync GraphQL-API Erfordern Sie die Erlaubnis, eine AWS WAF `ListResourcesForWebACL` Web-ACL aufzurufen.

```
{
  "Sid": "ListResourcesForWebACL",
  "Effect": "Allow",
  "Action": [
    "wafv2:ListResourcesForWebACL"
  ],
  "Resource": [
    "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
  ]
}
```

Amazon-Cognito-Benutzerpool

Erfordert die Erlaubnis, die Amazon Cognito `ListResourcesForWebACL` Cognito-Aktion für den Ressourcentyp des Benutzerpools aufzurufen und aufzurufen 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 Dienst

Erfordert die Erlaubnis, die App `ListAssociatedServicesForWebAcl` Runner-Aktion für den App Runner-Dienstressourcentyp aufzurufen und aufzurufen 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 Verifizierte Access-Instanz

Erfordert die Erlaubnis, die `ec2:DescribeVerifiedAccessInstanceWebAclAssociations` Aktion für den Ressourcentyp „Verified Access“ aufzurufen und aufzurufen 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/*"
    ]
}

```

Politische Ressourcen für AWS WAF

Unterstützt Richtlinienressourcen

Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein `Resource` oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen [Amazon-Ressourcennamen \(ARN\)](#) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"

```

Eine Liste der AWS WAF Ressourcentypen und ihrer ARNs finden Sie unter [Von AWS WAF V2 definierte Ressourcen](#) in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN jeder Ressource angeben können, finden Sie unter [Von AWS WAF V2 definierte Aktionen](#). Um den Zugriff auf eine Teilmenge von AWS WAF Ressourcen zu erlauben oder zu verweigern, nehmen Sie den ARN der Ressource in das `resource` Element Ihrer Richtlinie auf.

Die ARNs von AWS WAF `wafv2` Ressourcen haben das folgende Format:

```
arn:partition:wafv2:region:account-id:scope/resource-type/resource-name/resource-id
```

Allgemeine Informationen zu ARN-Spezifikationen finden Sie unter [Amazon Resource Names \(ARNs\)](#) in der Allgemeine Amazon Web Services-Referenz.

Im Folgenden sind die spezifischen Anforderungen für die ARNs von `wafv2` Ressourcen aufgeführt:

- **Region:** Für AWS WAF Ressourcen, die Sie zum Schutz von CloudFront Amazon-Distributionen verwenden, setzen Sie diesen Wert auf `us-east-1`. Andernfalls legen Sie hier die Region fest, die Sie mit Ihren geschützten regionalen Ressourcen verwenden.
- **Umfang:** Legen Sie den Geltungsbereich auf `global` für die Verwendung mit einer CloudFront Amazon-Distribution oder `regional` für die Verwendung mit einer der regionalen Ressourcen fest, die dies AWS WAF unterstützen. Bei den regionalen Ressourcen handelt es sich um eine Amazon API Gateway Gateway-REST-API, einen Application Load Balancer, eine AWS AppSync GraphQL-API, einen Amazon Cognito Cognito-Benutzerpool, einen AWS App Runner Service und eine AWS Verified Access-Instance.
- **Ressourcentyp:** Geben Sie einen der folgenden Werte an: `webacl`, `rulegroup` oder `ipset`, `regexpatternset` oder `managedruleset`.
- **Ressourcename:** Geben Sie den Namen an, den Sie der AWS WAF Ressource gegeben haben, oder geben Sie einen Platzhalter (*) an, um alle Ressourcen anzugeben, die die anderen Spezifikationen im ARN erfüllen. Sie müssen entweder den Ressourcennamen und die Ressourcen-ID oder einen Platzhalter für beide angeben.
- **resource-id:** Geben Sie die ID der AWS WAF Ressource an, oder geben Sie einen Platzhalter (*) an, um alle Ressourcen anzugeben, die die anderen Spezifikationen im ARN erfüllen. Sie müssen entweder den Ressourcennamen und die Ressourcen-ID oder für beide einen Platzhalter angeben.

Der folgende ARN gibt zum Beispiel alle Web-ACLs mit regionalem Geltungsbereich für das Konto 111122223333 in Region `us-west-1` an:

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

Der folgende ARN gibt die Regelgruppe MyIPManagementRuleGroup mit dem globalen Geltungsbereich für das Konto 111122223333 in Region us-east-1:

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

Beispiele für AWS WAF identitätsbasierte Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS WAF](#)

Bedingungsschlüssel für Richtlinien für AWS WAF

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Ja
---	----

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition block`) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die [Bedingungsoperatoren](#) verwenden, z. B. `ist gleich` oder `kleiner als`, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen OR Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter [IAM-Richtlinienelemente: Variablen und Tags](#) im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [Kontextschlüssel für AWS globale Bedingungen](#) im IAM-Benutzerhandbuch.

AWS WAF Unterstützt außerdem die folgenden Bedingungsschlüssel, mit denen Sie Ihre IAM-Richtlinien detailliert filtern können:

- wafv2: LogDestinationResource

Dieser Bedingungsschlüssel verwendet eine Amazon Resource Name (ARN) -Spezifikation für das Protokollierungsziel. Dies ist der ARN, den Sie für das Protokollierungsziel angeben, wenn Sie den REST-API-Aufruf verwenden `PutLoggingConfiguration`.

Sie können explizit einen ARN angeben und Sie können die Filterung für den ARN angeben. Das folgende Beispiel spezifiziert die Filterung nach Amazon S3 S3-Bucket-ARNs, die einen bestimmten Standort und ein bestimmtes Präfix haben.

```
"Condition": { "ArnLike": { "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-suffix/custom-prefix/*" } }
```

- wafv2: LogScope

Dieser Bedingungsschlüssel definiert die Quelle der Protokollierungskonfiguration in einer Zeichenfolge. Derzeit ist dies immer auf den Standardwert von `customer`, was darauf hinweist, dass das Protokollierungsziel Ihnen gehört und von Ihnen verwaltet wird.

Eine Liste der AWS WAF Bedingungsschlüssel finden Sie unter [Bedingungsschlüssel für AWS WAF V2](#) in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter [Von AWS WAF V2 definierte Aktionen](#).

Beispiele für AWS WAF identitätsbasierte Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS WAF](#)

ACLs in AWS WAF

Unterstützt ACLs

Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit AWS WAF

Unterstützt ABAC (Tags in Richtlinien)

Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement einer [Richtlinie Tag-Informationen](#) an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter [Was ist ABAC?](#) im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe [Attributbasierte Zugriffskontrolle \(ABAC\)](#) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit AWS WAF

Unterstützt temporäre Anmeldeinformationen

Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären

Anmeldeinformationen AWS-Services [funktionieren AWS-Services](#) , [finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM](#).

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter [Wechseln zu einer Rolle \(Konsole\)](#) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter [Temporäre Sicherheitsanmeldeinformationen in IAM](#).

Zugriffssitzungen für den Service weiterleiten AWS WAF

Unterstützt Forward Access Sessions (FAS)	Ja
---	----

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

Servicerollen für AWS WAF

Unterstützt Servicerollen	Ja
---------------------------	----

Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern

und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.

Warning

Durch das Ändern der Berechtigungen für eine Servicerolle kann die AWS WAF Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, AWS WAF wenn Sie dazu eine Anleitung erhalten.

Dienstbezogene Rollen für AWS WAF

Unterstützt serviceverknüpfte Rollen	Ja
--------------------------------------	----

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von AWS WAF dienstbezogenen Rollen finden Sie unter [Verwenden von serviceverknüpften Rollen für AWS WAF](#)

Beispiele für identitätsbasierte Richtlinien für AWS WAF

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, AWS WAF -Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von definiert wurden AWS WAF, einschließlich des Formats der ARNs für jeden der Ressourcentypen, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS WAF V2](#) in der Service Authorization Reference.

Themen

- [Bewährte Methoden für Richtlinien](#)
- [Verwenden der AWS WAF -Konsole](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)
- [Gewähren Sie schreibgeschützten Zugriff auf, und AWS WAF CloudFront CloudWatch](#)
- [Gewähren Sie vollen Zugriff auf AWS WAF CloudFront, und CloudWatch](#)
- [Gewähren Sie Zugriff auf ein einzelnes AWS-Konto](#)
- [Gewähren Sie Zugriff auf eine einzelne Web-ACL](#)
- [CLI Zugriff auf eine Web-ACL und Regelgruppe gewähren](#)

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS WAF Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter [AWS -verwaltete Richtlinien](#) oder [AWS -verwaltete Richtlinien für Auftrags-Funktionen](#) im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten: Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter [Richtlinien und Berechtigungen in IAM](#) im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs: Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben,

um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: Bedingung](#) im IAM-Benutzerhandbuch.

- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten: IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter [Richtlinienvvalidierung zum IAM Access Analyzer](#) im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter [Konfigurieren eines MFA-geschützten API-Zugriffs](#) im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Bewährte Methoden für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

Verwenden der AWS WAF -Konsole

Um auf die AWS WAF Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS WAF Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die AWS WAF Konsole verwenden können, fügen Sie den Entitäten außerdem mindestens die AWS WAF `AWSWAFConsoleReadOnlyAccess` AWS verwaltete Richtlinie hinzu. Informationen zu dieser verwalteten Richtlinie finden Sie unter [AWS verwaltete Richtlinie: AWSWAFConsoleReadOnlyAccess](#). Weitere Informationen zum Anhängen

einer verwalteten Richtlinie an einen Benutzer finden Sie unter [Hinzufügen von Berechtigungen für einen Benutzer](#) im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API oder. AWS CLI AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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": "*"
    }
  ]
}
```

Gewähren Sie schreibgeschützten Zugriff auf, und AWS WAF CloudFront CloudWatch

Die folgende Richtlinie gewährt Benutzern nur Lesezugriff auf AWS WAF Ressourcen, CloudFront Amazon-Webverteilungen und Amazon-Metriken. CloudWatch Es ist nützlich für Benutzer, die die Erlaubnis benötigen, die Einstellungen in AWS WAF Bedingungen, Regeln und Web-ACLs einzusehen, um zu sehen, welche Distribution mit einer Web-ACL verknüpft ist, und um Metriken und eine Stichprobe von Anfragen in zu überwachen. CloudWatch Diese Benutzer können AWS WAF - Ressourcen nicht erstellen, aktualisieren oder löschen.

```
{
  "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": "*"
    }
  ]
}
```

Gewähren Sie vollen Zugriff auf AWS WAF CloudFront, und CloudWatch

Mit der folgenden Richtlinie können Benutzer jeden beliebigen AWS WAF Vorgang und jeden beliebigen Vorgang auf CloudFront Webverteilungen ausführen sowie Messwerte und eine Stichprobe von Anfragen in CloudWatch überwachen. Sie ist nützlich für Benutzer, die AWS WAF Administratoren sind.

```
{
  "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": "*"
}
]
}

```

Es wird dringend empfohlen, dass Sie die Multi-Factor Authentication (MFA, Multifaktor-Authentifizierung) für Benutzer mit Administrator-Berechtigungen konfigurieren. Weitere Informationen finden Sie unter [Verwenden von Geräten mit Multi-Factor Authentication \(MFA\) AWS](#) im IAM-Benutzerhandbuch.

Gewähren Sie Zugriff auf ein einzelnes AWS-Konto

Diese Richtlinie erteilt die folgenden Berechtigungen für das Konto 444455556666:

- Voller Zugriff auf alle AWS WAF Abläufe und Ressourcen.
- Lese- und Aktualisierungszugriff auf alle CloudFront Distributionen, sodass Sie Web-ACLs und CloudFront Distributionen zuordnen können.
- Lesezugriff auf alle CloudWatch Metriken und Metrikstatistiken, sodass Sie CloudWatch Daten und eine Stichprobe von Anfragen in der Konsole anzeigen können. 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": [
      "*"
    ]
  }
]
}

```

Gewähren Sie Zugriff auf eine einzelne Web-ACL

Mit der folgenden Richtlinie können Benutzer alle AWS WAF Vorgänge über die Konsole an einer bestimmten Web-ACL im Konto ausführen444455556666.

```

{
  "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": [
            "*"
        ]
    }
]
}

```

CLI Zugriff auf eine Web-ACL und Regelgruppe gewähren

Mit der folgenden Richtlinie können Benutzer jeden AWS WAF Vorgang über die CLI an einer bestimmten Web-ACL und einer bestimmten Regelgruppe im Konto ausführen444455556666.

```

{
  "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"
      ]
    }
  ]
}

```

Mit der folgenden Richtlinie können Benutzer alle AWS WAF Vorgänge über die Konsole an einer bestimmten Web-ACL im Konto ausführen444455556666.

```

{
  "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 verwaltete Richtlinien für AWS WAF

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie [kundenverwaltete Richtlinien](#) definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter [Von AWS verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSWAFReadOnlyAccess

Diese Richtlinie gewährt nur Leseberechtigungen, mit denen Benutzer auf AWS WAF Ressourcen und Ressourcen für integrierte Dienste wie Amazon, Amazon API Gateway CloudFront, Application Load Balancer AWS AppSync, Amazon Cognito und Verified Access zugreifen können. AWS App Runner AWS Sie können diese Richtlinie an Ihre IAM-Identitäten anhängen. AWS WAF ordnet diese Richtlinie auch einer Servicerolle zu, mit der Sie Aktionen AWS WAF in Ihrem Namen ausführen können.

Einzelheiten zu dieser Richtlinie finden Sie unter [AWSWAFReadOnlyAccess](#) in der IAM-Konsole.

AWS verwaltete Richtlinie: AWSWAFFullAccess

Diese Richtlinie gewährt vollen Zugriff auf AWS WAF Ressourcen und Ressourcen für integrierte Dienste wie Amazon CloudFront, Amazon API Gateway, Application Load Balancer AWS AppSync, Amazon Cognito und AWS Verified Access. AWS App Runner Sie können diese Richtlinie an Ihre IAM-Identitäten anhängen. AWS WAF ordnet diese Richtlinie auch einer Servicerolle zu, mit der Sie Aktionen AWS WAF in Ihrem Namen ausführen können.

Einzelheiten zu dieser Richtlinie finden Sie unter [AWSWAFFullAccess](#) in der IAM-Konsole.

AWS verwaltete Richtlinie: AWSWAFConsoleReadOnlyAccess

Diese Richtlinie gewährt der AWS WAF Konsole, die Ressourcen für AWS WAF und für integrierte Dienste wie Amazon, Amazon API Gateway, Application Load Balancer CloudFront, Amazon Cognito und Verified Access umfasst AWS AppSync, nur Leseberechtigungen. AWS App Runner AWS Sie können diese Richtlinie an Ihre IAM-Identitäten anhängen. AWS WAF ordnet diese Richtlinie auch einer Servicerolle zu, mit der Sie Aktionen AWS WAF in Ihrem Namen ausführen können.

Einzelheiten zu dieser Richtlinie finden Sie unter [AWSWAFConsoleReadOnlyAccess](#) in der IAM-Konsole.

AWS verwaltete Richtlinie: AWSWAFConsoleFullAccess

Diese Richtlinie gewährt vollen Zugriff auf die AWS WAF Konsole, die Ressourcen für AWS WAF und für integrierte Dienste wie Amazon, Amazon API Gateway CloudFront, Application Load Balancer AWS AppSync, Amazon Cognito und AWS Verified Access umfasst. AWS App Runner Sie können diese Richtlinie an Ihre IAM-Identitäten anhängen. AWS WAF ordnet diese Richtlinie auch einer Servicerolle zu, mit der Sie Aktionen AWS WAF in Ihrem Namen ausführen können.

Einzelheiten zu dieser Richtlinie finden Sie unter [AWSWAFConsoleFullAccess](#) in der IAM-Konsole.

AWS WAF Aktualisierungen der AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen der AWS verwalteten Richtlinien AWS WAF seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst. Wenn Sie automatische Benachrichtigungen über Änderungen an dieser Seite erhalten möchten, abonnieren Sie den RSS-Feed auf der Seite mit dem AWS WAF Dokumentenverlauf unter [Dokumentverlauf](#).

Richtlinie	Beschreibung der Änderung	Datum
<p>AWSWAFFullAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Ressourcen in Ihrem Namen in AWS WAF und in integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFFullAccess.</p>	<p>Erweiterte Berechtigungen zum Hinzufügen von Instanzen mit AWS verifiziertem Zugriff zu den Ressourcentypen, mit AWS WAF denen Sie sich schützen können.</p>	2023-06-17
<p>AWSWAFReadOnlyAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Ressourcen in Ihrem Namen in AWS WAF und in integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFReadOnlyAccess.</p>	<p>Erweiterte Berechtigungen zum Hinzufügen von Instanzen mit AWS verifiziertem Zugriff zu den Ressourcentypen, mit AWS WAF denen Sie sich schützen können.</p>	2023-06-17
<p>AWSWAFConsoleFullAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Konsolenressourcen und anderen AWS Ressourcen in</p>	<p>Erweiterte Berechtigungen zum Hinzufügen von Instanzen mit AWS verifiziertem Zugriff zu den Ressourcentypen, mit AWS WAF denen Sie sich schützen können.</p>	2023-06-17

Richtlinie	Beschreibung der Änderung	Datum
<p>Ihrem Namen in AWS WAF und in integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFConsoleFullAccess.</p>		
<p><code>AWSWAFConsoleReadOnlyAccess</code></p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Konsolenressourcen und anderen AWS Ressourcen in Ihrem Namen in AWS WAF und in integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFConsoleReadOnlyAccess.</p>	<p>Erweiterte Berechtigungen zum Hinzufügen von Instanzen mit AWS verifiziertem Zugriff zu den Ressourcentypen, mit AWS WAF denen Sie sich schützen können.</p>	2023-06-17
<p><code>AWSWAFFullAccess</code></p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Ressourcen in Ihrem Namen in AWS WAF und in integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFFullAccess.</p>	<p>Erweiterte Berechtigungen zur Korrektur der Zugriffseinstellungen für AWS App Runner Dienste.</p>	2023-06-06

Richtlinie	Beschreibung der Änderung	Datum
<p>AWSWAFReadOnlyAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Ressourcen in Ihrem Namen in und in AWS WAF integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFReadOnlyAccess.</p>	<p>Erweiterte Berechtigungen zur Korrektur der Zugriffseinstellungen für AWS App Runner Dienste.</p>	2023-06-06
<p>AWSWAFConsoleFullAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Konsolenressourcen und anderen AWS Ressourcen in Ihrem Namen in und in AWS WAF integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFConsoleFullAccess.</p>	<p>Erweiterte Berechtigungen zur Korrektur der Zugriffseinstellungen für AWS App Runner Dienste.</p>	2023-06-06
<p>AWSWAFConsoleReadOnlyAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Konsolenressourcen und anderen AWS Ressourcen in Ihrem Namen in und in AWS WAF integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFConsoleReadOnlyAccess.</p>	<p>Erweiterte Berechtigungen zur Korrektur der Zugriffseinstellungen für AWS App Runner Dienste.</p>	2023-06-06

Richtlinie	Beschreibung der Änderung	Datum
<p>AWSWAFFullAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Ressourcen in Ihrem Namen in und in AWS WAF integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFFullAccess.</p>	<p>Erweiterte Berechtigungen zum Hinzufügen von AWS App Runner Diensten zu den Ressourcentypen, mit AWS WAF denen Sie sich schützen können.</p>	2023-03-30
<p>AWSWAFReadOnlyAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Ressourcen in Ihrem Namen in AWS WAF und in integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFReadOnlyAccess.</p>	<p>Erweiterte Berechtigungen zum Hinzufügen von AWS App Runner Diensten zu den Ressourcentypen, mit AWS WAF denen Sie sich schützen können.</p>	2023-03-30
<p>AWSWAFConsoleFullAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Konsolenressourcen und anderen AWS Ressourcen in Ihrem Namen in AWS WAF und in integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFConsoleFullAccess.</p>	<p>Erweiterte Berechtigungen zum Hinzufügen von AWS App Runner Diensten zu den Ressourcentypen, mit AWS WAF denen Sie sich schützen können.</p>	2023-03-30

Richtlinie	Beschreibung der Änderung	Datum
<p>AWSWAFConsoleReadOnlyAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Konsolenressourcen und anderen AWS Ressourcen in Ihrem Namen in AWS WAF und in integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFConsoleReadOnlyAccess.</p>	<p>Erweiterte Berechtigungen zum Hinzufügen von AWS App Runner Diensten zu den Ressourcentypen, mit AWS WAF denen Sie sich schützen können.</p>	2023-03-30
<p>AWSWAFFullAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Ressourcen in Ihrem Namen in AWS WAF und in integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFFullAccess.</p>	<p>Erweiterte Berechtigungen zum Hinzufügen von Amazon Cognito Cognito-Benutzerpools zu den Ressourcentypen, mit AWS WAF denen Sie sich schützen können.</p>	25.08.2022
<p>AWSWAFReadOnlyAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Ressourcen in Ihrem Namen in AWS WAF und in integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFReadOnlyAccess.</p>	<p>Erweiterte Berechtigungen zum Hinzufügen von Amazon Cognito Cognito-Benutzerpools zu den Ressourcentypen, mit AWS WAF denen Sie sich schützen können.</p>	25.08.2022

Richtlinie	Beschreibung der Änderung	Datum
<p>AWSWAFConsoleFullAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Konsolenressourcen und anderen AWS Ressourcen in Ihrem Namen in AWS WAF und in integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFConsoleFullAccess.</p>	<p>Erweiterte Berechtigungen zum Hinzufügen von Amazon Cognito Cognito-Benutzerpools zu den Ressourcentypen, mit AWS WAF denen Sie sich schützen können.</p>	25.08.2022
<p>AWSWAFConsoleReadOnlyAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Konsolenressourcen und anderen AWS Ressourcen in Ihrem Namen in AWS WAF und in integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFConsoleReadOnlyAccess.</p>	<p>Erweiterte Berechtigungen zum Hinzufügen von Amazon Cognito Cognito-Benutzerpools zu den Ressourcentypen, mit AWS WAF denen Sie sich schützen können.</p>	25.08.2022

Richtlinie	Beschreibung der Änderung	Datum
<p>AWSWAFFullAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Ressourcen in Ihrem Namen in AWS WAF und in integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFFullAccess.</p>	<p>Die Berechtigungseinstellungen für die Protokollzustellung für Amazon Simple Storage Service (Amazon S3) und Amazon CloudWatch Logs wurden korrigiert. Diese Änderung behebt Zugriffsverweigerungsfehler, die während der Protokollierungskonfiguration auftraten. Weitere Informationen zum Protokollieren Ihres Web-ACL-Datenverkehrs finden Sie unter AWS WAF Web-ACL-Verkehr protokollieren.</p>	11.01.2022
<p>AWSWAFConsoleFullAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Konsolenressourcen und anderen AWS Ressourcen in Ihrem Namen in AWS WAF und in integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFConsoleFullAccess.</p>	<p>Die Berechtigungseinstellungen für die Protokollzustellung für Amazon Simple Storage Service (Amazon S3) und Amazon CloudWatch Logs wurden korrigiert. Diese Änderung behebt Zugriffsfehler, die während der Protokollierungskonfiguration aufgetreten sind. Weitere Informationen zum Protokollieren Ihres Web-ACL-Datenverkehrs finden Sie unter AWS WAF Web-ACL-Verkehr protokollieren.</p>	11.01.2022

Richtlinie	Beschreibung der Änderung	Datum
<p>AWSWAFFullAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Ressourcen in Ihrem Namen in AWS WAF und in integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFFullAccess.</p>	<p>Neue Berechtigungen für erweiterte Protokollierungsoptionen wurden hinzugefügt.</p> <p>Diese Änderung ermöglicht den AWS WAF Zugriff auf die zusätzlichen Protokollierungsziele Amazon Simple Storage Service (Amazon S3) und Amazon CloudWatch Logs. Weitere Informationen zum Protokollieren Ihres Web-ACL-Datenverkehrs finden Sie unter AWS WAF Web-ACL-Verkehr protokollieren.</p>	15.11.2021
<p>AWSWAFConsoleFullAccess</p> <p>Diese Richtlinie ermöglicht AWS WAF die Verwaltung von AWS Konsolenressourcen und anderen AWS Ressourcen in Ihrem Namen in AWS WAF und in integrierten Diensten.</p> <p>Details in der IAM-Konsole: AWSWAFConsoleFullAccess.</p>	<p>Neue Berechtigungen für erweiterte Protokollierungsoptionen wurden hinzugefügt.</p> <p>Diese Änderung ermöglicht den AWS WAF Zugriff auf die zusätzlichen Protokollierungsziele Amazon Simple Storage Service (Amazon S3) und Amazon CloudWatch Logs. Weitere Informationen zum Protokollieren Ihres Web-ACL-Datenverkehrs finden Sie unter AWS WAF Web-ACL-Verkehr protokollieren.</p>	15.11.2021

Richtlinie	Beschreibung der Änderung	Datum
AWS WAF hat begonnen, Änderungen zu verfolgen	AWS WAF hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	2021-3-01

Fehlerbehebung bei AWS WAF Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS WAF und IAM auftreten können.

Themen

- [Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS WAF](#)
- [Ich bin nicht berechtigt, iam auszuführen: PassRole](#)
- [Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS WAF Ressourcen ermöglichen](#)

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS WAF

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven `my-example-widget`-Ressource anzuzeigen, jedoch nicht über `wafv2:GetWidget`-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
wafv2:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `wafv2:GetWidget`-Aktion auf die `my-example-widget`-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an AWS WAF übergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS WAF auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS WAF Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffssteuerungslisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen AWS WAF unterstützt werden, finden Sie unter [Wie AWS WAF funktioniert mit IAM](#).
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter [Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto, den Sie besitzen](#).

- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter [Gewähren von Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien](#) im IAM-Benutzerhandbuch.

Verwenden von serviceverknüpften Rollen für AWS WAF

AWS WAF verwendet AWS Identity and Access Management (IAM) [serviceverknüpfte](#) Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. AWS WAF Mit Diensten verknüpfte Rollen sind vordefiniert AWS WAF und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle AWS WAF erleichtert die Einrichtung, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS WAF definiert die Berechtigungen ihrer dienstbezogenen Rollen und AWS WAF kann, sofern nicht anders definiert, nur ihre Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann an keine andere IAM-Entität angefügt werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem die zugehörigen Ressourcen gelöscht wurden. Dadurch werden Ihre AWS WAF Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Informationen zu anderen Services, die serviceverknüpften Rollen unterstützen, finden Sie unter [AWS -Services, die mit IAM funktionieren](#). Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für AWS WAF

AWS WAF verwendet die serviceverknüpfte Rolle. `AWSServiceRoleForWAFV2Logging`

AWS WAF verwendet diese serviceverknüpfte Rolle, um Protokolle in Amazon Data Firehose zu schreiben. Diese Rolle wird nur verwendet, wenn Sie die Anmeldung aktivieren. AWS WAF Weitere Informationen finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).

Die serviceverknüpfte Rolle `AWSServiceRoleForWAFV2Logging` vertraut dem Service `wafv2.amazonaws.com`, sodass dieser die Rolle annehmen kann.

Die Berechtigungsrichtlinien der Rolle AWS WAF ermöglichen es, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: `firehose:PutRecord` und `firehose:PutRecordBatch` auf Amazon Data Firehose Datenstream-Ressourcen mit einem Namen, der mit "aws-waf-logs-" beginnt. z. B. `aws-waf-logs-us-east-2-analytics`.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [serviceverknüpfte Rollenberechtigungen](#) im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für AWS WAF

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie die AWS WAF AWS Management Console Anmeldung aktivieren oder eine `PutLoggingConfiguration` Anfrage in der AWS WAF CLI oder der AWS WAF API stellen, AWS WAF wird die serviceverknüpfte Rolle für Sie erstellt.

Sie müssen über die `iam:CreateServiceLinkedRole`-Berechtigung verfügen, um die Protokollierung zu aktivieren.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie die AWS WAF Protokollierung aktivieren, AWS WAF wird die dienstbezogene Rolle erneut für Sie erstellt.


Bearbeiten einer serviceverknüpften Rolle für AWS WAF

AWS WAF erlaubt es Ihnen nicht, die `AWSServiceRoleForWAFV2Logging` dienstverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für AWS WAF

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte

juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpften Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

 Note

Wenn der AWS WAF Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um AWS WAF Ressourcen zu löschen, die verwendet werden von

AWSServiceRoleForWAFV2Logging

1. Entfernen Sie auf der AWS WAF Konsole die Protokollierung aus jeder Web-ACL. Weitere Informationen finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).
2. Senden Sie über die API oder CLI eine DeleteLoggingConfiguration-Anforderung für jede Web-ACL, für die die Protokollierung aktiviert ist. Weitere Informationen finden Sie unter [AWS WAF -API-Referenz](#).

So löschen Sie die serviceverknüpfte Rolle mit IAM

Sie können die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden, um die AWSServiceRoleForWAFV2Logging-serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Leitfaden.

Unterstützte Regionen für serviceverknüpfte AWS WAF -Rollen

AWS WAF unterstützt die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter [AWS WAF Endpunkte und -Kontingente](#).

Einloggen und Überwachen AWS WAF

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit AWS WAF und Leistung Ihrer AWS Lösungen. Sie sollten Überwachungsdaten aus allen Teilen Ihrer AWS Lösung sammeln, damit Sie einen etwaigen Ausfall an mehreren Stellen leichter debuggen können. AWS bietet mehrere Tools zur Überwachung Ihrer AWS WAF Ressourcen und zur Reaktion auf potenzielle Ereignisse:

CloudWatch Amazon-Alarme

Mithilfe von CloudWatch Alarmen beobachten Sie eine einzelne Metrik über einen von Ihnen festgelegten Zeitraum. Wenn die Metrik einen bestimmten Schwellenwert überschreitet, CloudWatch sendet eine Benachrichtigung an ein Amazon SNS SNS-Thema oder eine AWS Auto Scaling Richtlinie. Weitere Informationen finden Sie unter [Überwachung mit Amazon CloudWatch](#).

AWS CloudTrail protokolliert

CloudTrail bietet eine Aufzeichnung der Aktionen, die von einem Benutzer, einer Rolle oder einem AWS Dienst in ausgeführt wurden AWS WAF. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, an die die Anfrage gestellt wurde AWS WAF, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Informationen ermitteln. Weitere Informationen finden Sie unter [Protokollierung von AWS CloudTrail-API-Aufrufen mit](#).

AWS WAF Protokollierung des Web-ACL-Datenverkehrs

AWS WAF bietet die Protokollierung des Datenverkehrs, den Ihre Web-ACLs analysieren. Die Protokolle enthalten Informationen wie die Uhrzeit, zu der die Anfrage von Ihrer geschützten AWS Ressource AWS WAF empfangen wurde, detaillierte Informationen über die Anfrage und die Aktionseinstellung für die Regel, der die Anfrage entsprach. Weitere Informationen finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).

Konformitätsvalidierung für AWS WAF

Informationen darüber, ob AWS-Service ein [AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter](#) . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter [AWS Compliance-Programme AWS](#) .

Sie können Prüfberichte von Drittanbietern unter heruntergeladen AWS Artifact. Weitere Informationen finden Sie unter [Berichte heruntergeladen unter](#) .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- [Schnellstartanleitungen zu Sicherheit und Compliance](#) — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

Note

AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der [Referenz für HIPAA-berechtigte Services](#).

- [AWS Compliance-Ressourcen](#) — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- [AWS Leitfäden zur Einhaltung von Vorschriften für Kunden](#) — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- [Evaluierung von Ressourcen anhand von Regeln](#) im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.

- [AWS Security Hub](#)— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der [Security-Hub-Steuerungsreferenz](#).
- [AWS Audit Manager](#)— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz in AWS WAF

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter [AWS Globale](#) Infrastruktur.

Sicherheit der Infrastruktur in AWS WAF

Als verwalteter Dienst AWS WAF ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter [AWS Cloud-Sicherheit](#). Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff AWS WAF über das Netzwerk. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit [AWS Security Token Service](#) (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

AWS WAF Kontingente

Note

Dies ist die neueste Version von AWS WAF. Informationen zu AWS WAF Classic finden Sie unter [AWS WAF Klassisch](#).

AWS WAF unterliegt den folgenden Kontingenten (früher als Beschränkungen bezeichnet). Diese Kontingente sind für alle Regionen, in denen verfügbar AWS WAF ist, gleich. Für jede Region gelten diese Kontingente einzeln, die Kontingente können nicht über die Regionen kumuliert werden.

AWS WAF hat Standardkontingente für die maximale Anzahl von Entitäten, die Sie pro Konto haben können. Sie können [eine Erhöhung dieser Kontingente beantragen](#).

Ressource	Standardkontingent pro Konto und Region
Maximale Anzahl von Web-ACLs	100
Maximale Anzahl von Regelgruppen	100
Maximale Anzahl von IP-Sätzen	100
Maximale Anzahl von Anforderungen pro Sekunde pro Web-ACL	25,000
Maximale Anzahl von benutzerdefinierten Anforderungskopfzeilen pro Web-ACL oder Regelgruppe	100
Maximale Anzahl benutzerdefinierter Antwortkopfzeilen pro Web-ACL oder Regelgruppe	100
Maximale Anzahl benutzerdefinierter Antworttexte pro Web-ACL oder Regelgruppe	50
Maximale Anzahl von Tokendomänen in einer Liste von Web-ACL-Tokendomänen	10

Die maximal zulässige Anzahl von Anfragen pro Sekunde (RPS) CloudFront wird AWS WAF im Developer Guide festgelegt CloudFront und im [CloudFront Developer Guide](#) beschrieben.

AWS WAF hat feste Kontingente für die folgenden Entitätseinstellungen pro Konto und Region. Diese Kontingente können nicht geändert werden.

Ressource	Kontingente pro Konto und Region
Maximale Web-ACL-Kapazitätseinheiten (WCUs) pro Web-ACL*	5,000
Maximale WCUs pro Regelgruppe	5,000
Maximale Anzahl von Referenzanweisungen pro Regelgruppe. In einer Regelgruppe kann eine Referenzanweisung auf einen IP-Satz oder einen Regex-Mustersatz verweisen.	50
Maximale Anzahl von Referenzanweisungen pro Web-ACL. In einer Web-ACL kann eine Referenzanweisung auf eine Regelgruppe, einen IP-Satz oder einen Regex-Mustersatz verweisen.	50
Maximale Anzahl von IP-Adressen in CIDR-Notation pro IP-Satz	10.000
Maximale Anzahl von ratenbasierten Regeln pro Web-ACL	10
Maximale Anzahl von ratenbasierten Regeln pro Regelgruppe	4
Mindestanforderungsrate, die für eine ratebasierte Regel definiert werden kann	100
Maximale Anzahl eindeutiger IP-Adressen, die pro ratenbasierter Regel ratenbegrenzt werden können	10.000
Maximale Anzahl der Zeichen für eine Zeichenfolgen-Übereinstimmungsanweisung	200
Maximale Anzahl der Zeichen in jedem RegEx-Muster	200
Maximale Anzahl einzigartiger RegEx-Muster pro RegEx-Set	10

Ressource	Kontingente pro Konto und Region
Maximale Anzahl von RegEx-Sets	10
Maximale Größe eines Webanforderungstexts, der auf Application Load Balancer und AWS AppSync Schutzmaßnahmen überprüft werden kann	8 KB
Maximale Größe eines Webanfragetextes, auf den geprüft werden kann CloudFront, Schutzmaßnahmen für API Gateway, Amazon Cognito, App Runner und Verified Access**	64 KB
Maximale Anzahl von Texttransformationen pro Regelanweisung	10
Maximale Größe des benutzerdefinierten Antworttextes für eine einzelne benutzerdefinierte Antwortdefinition	4 KB
Maximale Anzahl an benutzerdefinierten Kopfzeilen für eine einzelne benutzerdefinierte Antwortdefinition	10
Maximale Anzahl an benutzerdefinierten Kopfzeilen für eine einzelne benutzerdefinierte Anforderungsdefinition	10
Maximale kombinierte Größe aller Antworttextinhalte für eine einzelne Regelgruppe oder eine einzelne Web-ACL	50 KB

*Bei der Verwendung von mehr als 1.500 WCUs in einer Web-ACL fallen Kosten an, die über den Basispreis für Web-ACL hinausgehen. Weitere Informationen finden Sie unter [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#) und [Preise zu AWS WAF](#).

**Standardmäßig ist das Limit für Body Inspection für API Gateway-CloudFront, Amazon Cognito-, App Runner- und Verified Access-Ressourcen auf 16 KB festgelegt. Sie können dieses Limit für jede dieser Ressourcen in Ihrer Web-ACL-Konfiguration jedoch bis zum angegebenen Maximum erhöhen. Weitere Informationen finden Sie unter [Verwaltung der Größenbeschränkungen bei Körperinspektionen](#).

AWS WAF hat die folgenden festen Kontingente für Anrufe pro Konto und Region. Diese Kontingente gelten für die gesamten Aufrufe an den Dienst über alle verfügbaren Mittel, einschließlich der

Konsole, CLI, AWS CloudFormation, der REST-API und der SDKs. Diese Kontingente können nicht geändert werden.

Art des Anrufs	Kontingente pro Konto und Region
Maximale Anzahl von Aufrufen an <code>AssociateWebACL</code>	Eine einzelne Anfrage alle 2 Sekunden
Maximale Anzahl von Aufrufen an <code>DisassociateWebACL</code>	Eine einzelne Anfrage alle 2 Sekunden
Maximale Anzahl von Aufrufen an <code>GetWebACLForResource</code>	Eine einzelne Anfrage pro Sekunde
Maximale Anzahl von Aufrufen an <code>ListResourcesForWebACL</code>	Eine einzelne Anfrage pro Sekunde
Maximale Anzahl von Aufrufen einer einzelnen Get- oder List-Aktion, wenn kein anderes Kontingent dafür definiert ist	Fünf Anforderungen pro Sekunde
Maximale Anzahl von Aufrufen einer einzelnen Create-, Put- oder Update-Aktion, wenn kein anderes Kontingent dafür definiert ist	Eine einzelne Anfrage pro Sekunde

Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF

Dieser Abschnitt enthält Anleitungen für die Migration Ihrer Regeln und Web-ACLs von AWS WAF Classic zu AWS WAF. AWS WAF wurde im November 2019 veröffentlicht. Wenn Sie Ressourcen wie Regeln und Web-ACLs mit AWS WAF Classic erstellt haben, müssen Sie sie entweder mit AWS WAF Classic bearbeiten oder sie auf diese neueste Version migrieren.

Bevor Sie mit der Migration beginnen, sollten Sie sich mit diesen Informationen vertraut machen, AWS WAF indem Sie sie [AWS WAF](#) durchlesen.

Themen

- [Warum zu migrieren AWS WAF?](#)
- [So funktioniert die Migration](#)
- [Migrationsvorbehalte und -beschränkungen](#)
- [Migrieren einer Web-ACL von AWS WAF Classic zu AWS WAF](#)

Warum zu migrieren AWS WAF?

Die neueste Version von AWS WAF bietet viele Verbesserungen gegenüber der Vorgängerversion und behält gleichzeitig die meisten Konzepte und Terminologie bei, an die Sie gewöhnt sind.

Die folgende Liste beschreibt die wichtigsten Änderungen in der letzten AWS WAF. Bevor Sie mit der Migration fortfahren, nehmen Sie sich bitte etwas Zeit, um diese Liste zu lesen und sich mit dem Rest des AWS WAF Handbuchs vertraut zu machen.

- **AWS Verwaltete Regeln für AWS WAF** — Die Regelgruppen, die jetzt über AWS Verwaltete Regeln verfügbar sind, bieten Schutz vor gängigen Internet-Bedrohungen. Die meisten dieser Regelgruppen sind kostenlos in enthalten AWS WAF. Weitere Informationen finden Sie unter [AWS Liste der Regelgruppen für verwaltete Regeln](#) und im Blogbeitrag [Ankündigung AWS verwalteter Regeln für AWS WAF](#).
- **Neue AWS WAF API** — Mit der neuen API können Sie all Ihre AWS WAF Ressourcen mit einem einzigen Satz von APIs konfigurieren. Um zwischen regionalen und globalen Anwendungen zu unterscheiden, enthält die neue API eine scope-Einstellung. Weitere Informationen zur API finden Sie in den [AWS -WAFV2-Aktionen](#) und [AWS -WAFV2-Datentypen](#).

In den APIs, SDKs, CLIs und AWS WAF Classic behält Classic seine Benennungsschemata bei AWS CloudFormation, und auf diese neueste Version von AWS WAF wird je nach Kontext mit einem hinzugefügten V2 oder v2 verwiesen.

- **Vereinfachte Dienstkontingente (Limits)** — erlaubt AWS WAF jetzt mehr Regeln pro Web-ACL und ermöglicht es Ihnen, längere Regex-Muster auszudrücken. Weitere Informationen finden Sie unter [AWS WAF Kontingente](#).
- **Web-ACL-Grenzwerte basieren jetzt auf den Rechenanforderungen** — Web-ACL-Grenzwerte basieren jetzt auf Web-ACL-Kapazitätseinheiten (WCU). AWS WAF berechnet die WCU für eine

Regel anhand der Betriebskapazität, die für die Ausführung der Regel erforderlich ist. Die WCU einer Web-ACL ist die Summe der WCUs aller Regeln und Regelgruppen in der Web-ACL.

Allgemeine Informationen zu WCUs finden Sie unter [Wie AWS WAF funktioniert](#). Weitere Informationen zur WCU-Verwendung der einzelnen Regeln finden Sie unter [Grundlagen der Regelerklärung](#).

- Dokumentenbasiertes Schreiben von Regeln: Sie können jetzt Regeln, Regelgruppen und Web-ACLs im JSON-Format schreiben und ausdrücken. Sie müssen keine einzelnen API-Aufrufe mehr verwenden, um andere Bedingungen zu erstellen und dann die Bedingungen einer Regel zuzuordnen. Dies vereinfacht erheblich, wie Sie Ihren Code schreiben und pflegen. Sie können auf ein JSON-Format Ihrer Web-ACLs über die Konsole zugreifen, wenn Sie die Web-ACL anzeigen, indem Sie Download web ACL as JSON (Web-ACL als JSON herunterladen) auswählen. Wenn Sie eine eigene Regel erstellen, können Sie auf ihre JSON-Darstellung zugreifen, indem Sie den Rule JSON editor (Regel-JSON-Editor) auswählen.
- Regelverschachtelung und vollständige Unterstützung für logische Vorgänge: Sie können komplexe kombinierte Regeln schreiben, indem Sie logische Regelanweisungen verwenden und verschachteln. Sie können Anweisungen wie [A AND NOT(B OR C)] erstellen. Weitere Informationen finden Sie unter [Logische Regelaussagen](#).
- Verbesserte ratenbasierte Regeln — In der neuesten Version von können Sie das Zeitfenster AWS WAF, in dem die Regel ausgewertet, und die Art und Weise, wie die Regel Anfragen aggregiert, anpassen. Sie können die Aggregation mithilfe von Kombinationen verschiedener Merkmale von Webanfragen anpassen. Darüber hinaus reagieren die neuesten ratenbasierten Regeln schneller auf Verkehrsänderungen. Weitere Informationen finden Sie unter [Ratenbasierte Regelanweisung](#).
- Unterstützung variabler CIDR-Bereiche für IP-Set: IP-Set-Spezifikationen bieten jetzt mehr Flexibilität in den IP-Bereichen. Unterstützt für IPv4 bis. AWS WAF /1 /32 Für IPv6 AWS WAF unterstützt /1 bis. /128 Weitere Informationen zu IP-Sets finden Sie unter [IP-Set-Übereinstimmungsregelanweisung](#).
- Verkettbare Texttransformationen — Sie AWS WAF können mehrere Texttransformationen für den Inhalt von Webanfragen durchführen, bevor dieser überprüft wird. Weitere Informationen finden Sie unter [Texttransformationen](#).
- Verbessertes Konsolenerlebnis — Die neue AWS WAF Konsole bietet einen visuellen Regelgenerator und ein benutzerfreundlicheres Konsolendesign.
- Erweiterte Optionen für Firewall Manager AWS WAF Manager-Richtlinien — In der Firewall Manager Manager-Verwaltung von AWS WAF Web-ACLs können Sie jetzt eine Reihe von Regelgruppen erstellen, die zuerst AWS WAF verarbeitet werden, und eine Reihe von

Regelgruppen, die zuletzt AWS WAF verarbeitet werden. Nachdem Sie die AWS WAF Richtlinie angewendet haben, können lokale Kontoinhaber ihre eigenen Regelgruppen hinzufügen, die zwischen diesen beiden Gruppen AWS WAF verarbeitet werden. Weitere Informationen zu AWS WAF -Richtlinien in Firewall Manager finden Sie unter [AWS WAF Richtlinien](#).

- AWS CloudFormation Unterstützung für alle Arten von Regeln — AWS WAF AWS CloudFormation unterstützt alle Arten von Regeln, die von der AWS WAF Konsole und der API unterstützt werden. Darüber hinaus können Sie die Regeln, die Sie im JSON-Format schreiben, einfach in das YAML-Format konvertieren.

So funktioniert die Migration

Die automatisierte Migration übernimmt den Großteil Ihrer AWS WAF Classic-Web-ACL-Konfiguration, sodass einige Dinge übrig bleiben, die Sie manuell erledigen müssen.

Im Folgenden werden die allgemeinen Schritte zum Migrieren einer Web-ACL aufgeführt.


1. Bei der automatisierten Migration wird alles gelesen, was mit Ihrer vorhandenen Web-ACL zu tun hat, ohne etwas in AWS WAF Classic zu ändern oder zu löschen. Sie erstellt eine Darstellung der Web-ACL und der zugehörigen Ressourcen, die kompatibel mit ist AWS WAF. Es wird eine AWS CloudFormation -Vorlage für die neue Web-ACL generiert und in einem Amazon-S3-Bucket gespeichert.
2. Sie stellen die Vorlage in bereit AWS CloudFormation, um die Web-ACL und die zugehörigen Ressourcen in AWS WAF neu zu erstellen.
3. Sie überprüfen die Web-ACL und schließen die Migration manuell ab. Stellen Sie sicher, dass Ihre neue Web-ACL alle Vorteile der neuesten AWS WAF-Funktionen nutzt.
4. Sie schalten Ihre geschützten Ressourcen manuell auf die neue Web-ACL um.

Migrationsvorbehalte und -beschränkungen

Die Migration übernimmt nicht alle Einstellungen genau so, wie sie in AWS WAF Classic festgelegt sind. Einige Elemente, wie verwaltete Regeln, werden nicht genau zwischen den beiden Versionen zugeordnet. Andere Einstellungen, wie die Zuordnungen der Web-ACL zu geschützten AWS - Ressourcen, werden in der neuen Version zunächst deaktiviert, sodass Sie sie hinzufügen können, wenn Sie bereit sind.

In der folgenden Liste werden die Vorbehalte der Migration und alle Schritte beschrieben, die Sie als Reaktion ausführen möchten. Verwenden Sie diese Übersicht, um Ihre Migration zu planen. Die detaillierten Migrationsschritte führen Sie später durch die empfohlenen Risikominderungsschritte.

- Einzelkonto — Sie können nur AWS WAF Classic-Ressourcen für jedes Konto zu AWS WAF Ressourcen für dasselbe Konto migrieren.
- Verwaltete Regeln — Bei der Migration werden keine verwalteten Regeln von AWS Marketplace Verkäufern übernommen. Einige AWS Marketplace Verkäufer haben entsprechende verwaltete Regeln AWS WAF , für die Sie erneut ein Abonnement abschließen können. Bevor Sie dies tun, lesen Sie sich die AWS verwalteten Regeln durch, die in der neuesten Version von enthalten sind AWS WAF. Die meisten davon sind für AWS WAF Benutzer kostenlos. Weitere Informationen zu verwalteten Regeln finden Sie unter [Verwaltete Regelgruppen](#).
- Web-ACL-Zuordnungen: Die Migration führt keine Zuordnungen zwischen der Web-ACL und den geschützten Ressourcen durch. Dies ist Absicht, um eine Beeinträchtigung Ihres Produktions-Workloads zu vermeiden. Nachdem Sie überprüft haben, ob alles korrekt migriert wurde, ordnen Sie die neue Web-ACL Ihren Ressourcen zu.
- Protokollierung: Protokollierung ist für die migrierte Web-ACL standardmäßig deaktiviert. Dies ist beabsichtigt. Aktivieren Sie die Protokollierung, wenn Sie bereit sind, von AWS WAF Classic zu zu wechseln AWS WAF.
- AWS Firewall Manager Regelgruppen — Die Migration behandelt keine Regelgruppen, die von Firewall Manager verwaltet werden. Sie können eine Web-ACL migrieren, die von Firewall Manager verwaltet wird, aber die Regelgruppe wird nicht übernommen. Statt das Migrationstool für diese Web-ACLs zu verwenden, erstellen Sie die Richtlinie für das neue AWS WAF in Firewall Manager neu.

 Note

Die Regelgruppen, die Firewall Manager für AWS WAF Classic verwaltete, waren Firewall Manager Manager-Regelgruppen. In der neuen Version von AWS WAF sind die Regelgruppen AWS WAF Regelgruppen. Funktionell sind sie gleich.

- AWS WAF Sicherheitsautomatisierungen — Versuchen Sie nicht, [AWS WAF Sicherheitsautomatisierungen](#) zu migrieren. Die Migration konvertiert keine Lambda-Funktionen, die möglicherweise von den Automatisierungen verwendet werden. Wenn eine neue AWS WAF Sicherheitsautomatisierungslösung verfügbar ist, die mit der neuesten Version kompatibel ist AWS WAF, stellen Sie diese Lösung erneut bereit.

Migrieren einer Web-ACL von AWS WAF Classic zu AWS WAF

Um eine Web-ACL zu migrieren und dorthin zu wechseln, führen Sie die automatische Migration durch. Führen Sie dann eine Reihe von manuellen Schritten aus.

Themen

- [Migrieren einer Web-ACL: automatisierte Migration](#)
- [Migrieren einer Web-ACL: manuelle Nachverfolgung](#)
- [Migrieren einer Web-ACL: Weitere Überlegungen](#)
- [Migrieren einer Web-ACL: Umstellung](#)

Migrieren einer Web-ACL: automatisierte Migration

So migrieren Sie automatisch eine Web-ACL-Konfiguration von AWS WAF Classic zu AWS WAF

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie Zu AWS WAF Classic wechseln und überprüfen Sie Ihre Konfigurationseinstellungen für die Web-ACL. Notieren Sie sich die Einstellungen unter Berücksichtigung der im vorhergehenden Abschnitt ([Migrationsvorbehalte und -beschränkungen](#)) beschriebenen Einschränkungen und Einschränkungen.
3. Suchen Sie im Informationsdialog oben den Satz, der mit Migrate web ACLs (Migrieren von Web-ACLs) beginnt. Wählen Sie den Link zum migration wizard (Migrationsassistenten) aus. Dadurch wird der Migrationsassistent gestartet.

Wenn Sie den Informationsdialog nicht sehen, haben Sie ihn möglicherweise geschlossen, seit Sie die AWS WAF Classic-Konsole gestartet haben. Wählen Sie in der Navigationsleiste „Zu neu wechseln“ und AWS WAF dann „Zu AWS WAF Classic wechseln“. Der Informationsdialog sollte nun wieder angezeigt werden.

4. Wählen Sie die Web-ACL aus, die Sie migrieren möchten.
5. Geben Sie für die Migration configuration (Migrationskonfiguration) einen Amazon-S3-Bucket an, der für die Vorlage verwendet werden soll. Sie benötigen einen Amazon S3 S3-Bucket, der ordnungsgemäß für die Migrations-API konfiguriert ist, um die von ihr generierte AWS CloudFormation Vorlage zu speichern.

- Wenn der Bucket verschlüsselt ist, muss die Verschlüsselung Amazon S3 (SSE-S3)-Schlüssel verwenden. Die Migration unterstützt keine Verschlüsselung mit AWS Key Management Service (SSE-KMS-) Schlüsseln.
 - Der Bucket-Name muss mit `aws-waf-migration-` beginnen. z. B. `aws-waf-migration-my-web-acl`.
 - Der Bucket muss sich in der Region befinden, in der Sie die Vorlage bereitstellen. Beispielsweise müssen Sie für eine Web-ACL in `us-west-2` einen Amazon-S3-Bucket in `us-west-2` verwenden und Sie müssen den Vorlagenstapel in `us-west-2` bereitstellen.
6. Als S3 bucket policy (S3-Bucket-Richtlinie), wird empfohlen, die `Auto apply the bucket policy required for migration` (Für die Migration erforderliche Bucket-Richtlinie automatisch anwenden) auszuwählen. Wenn Sie den Bucket selbst verwalten möchten, müssen Sie die folgende Bucket-Richtlinie manuell anwenden:

- Für globale CloudFront Amazon-Anwendungen (`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>/
*"
    }
  ]
}
```

- Für regionale Amazon API Gateway- oder Application Load Balancer-Anwendungen (`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>/
*"
    }
]
}
```

- Wählen Sie bei Choose how to handle rules that cannot be migrated (Auswählen, wie Regeln behandelt werden, die nicht migriert werden können) entweder aus, die Regeln, die nicht migriert werden können, auszuschließen, oder die Migration zu beenden. Weitere Informationen zu Regeln, die nicht migriert werden können, finden Sie unter [Migrationsvorbehalte und -beschränkungen](#).
- Wählen Sie Weiter aus.
- Überprüfen Sie unter AWS CloudFormation Vorlage erstellen Ihre Einstellungen und wählen Sie dann AWS CloudFormation Vorlage erstellen aus, um den Migrationsprozess zu starten. Dies kann je nach Komplexität Ihrer Web-ACL einige Minuten dauern.
- Unter AWS CloudFormation Stack erstellen und ausführen, um die Migration abzuschließen, können Sie wählen, ob Sie in der AWS CloudFormation Konsole einen Stack aus der Vorlage erstellen und die neue Web-ACL und die zugehörigen Ressourcen erstellen möchten. Wählen Sie dazu AWS CloudFormation Stack erstellen aus.

Nachdem der automatische Migrationsprozess abgeschlossen ist, können Sie mit den nachfolgenden manuellen Schritten fortfahren. Siehe [Migrieren einer Web-ACL: manuelle Nachverfolgung](#).

Migrieren einer Web-ACL: manuelle Nachverfolgung

Nachdem die automatisierte Migration abgeschlossen ist, überprüfen Sie die neu erstellte Web-ACL und füllen Sie die Komponenten aus, die die Migration nicht für Sie herbeiführt. Im folgenden Verfahren werden die Aspekte der Web-ACL-Verwaltung behandelt, die von der Migration nicht verarbeitet werden. Die Liste finden Sie unter [Migrationsvorbehalte und -beschränkungen](#).

Abschluss der grundlegenden Migration – manuelle Schritte

- Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

2. Die Konsole sollte automatisch die neueste Version von verwenden AWS WAF. Um dies zu überprüfen, überprüfen Sie, ob im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird. Wenn die Option Zur neuen Version wechseln angezeigt wird AWS WAF, wählen Sie diese Option aus, um zur neuesten Version zu wechseln.
3. Wählen Sie im Navigationsbereich Web ACLs aus.
4. Suchen Sie auf der Seite der Web-ACLs die neue Web-ACL in der Liste für die Region, in der Sie sie erstellt haben. Wählen Sie den Namen der Web-ACL aus, um die Einstellungen für die Web-ACL aufzurufen.
5. Vergleichen Sie alle Einstellungen für die neue Web-ACL mit Ihrer vorherigen AWS WAF Classic-Web-ACL. Standardmäßig sind Protokollierung und geschützte Ressourcenzuordnungen deaktiviert. Sie aktivieren diese, wenn Sie zur Umstellung bereit sind.
6. Wenn Ihre AWS WAF Classic-Web-ACL eine ratenbasierte Regel mit einer Bedingung hatte, wurde die Bedingung bei der Migration nicht übernommen. Sie können der Regel in der neuen Web-ACL Bedingungen hinzufügen.
 - a. Wählen Sie auf der Seite mit den Web-ACL-Einstellungen die Registerkarte Rules (Regeln) aus.
 - b. Suchen Sie die ratenbasierte Regel in der Liste, wählen Sie sie aus und wählen Sie Edit (Bearbeiten) aus.
 - c. Wählen Sie unter Criteria to count request towards rate limit (Kriterien zur Einbeziehung der Anforderung zur Ratengrenze) die Option Only consider requests that match the criteria in a rule statement (Nur Anforderungen berücksichtigen, die den Kriterien in einer Regelanweisung entsprechen) aus und geben Sie dann Ihre zusätzlichen Kriterien ein. Sie können die Kriterien mithilfe einer beliebigen Regelanweisung hinzufügen, die verschachtelt werden kann, einschließlich logischer Anweisungen. Weitere Informationen zu Ihren Auswahlmöglichkeiten finden Sie unter [Ratenbasierte Regelanweisung](#).
7. Wenn Ihre AWS WAF Classic-Web-ACL über eine verwaltete Regelgruppe verfügte, wurde die Einbeziehung der Regelgruppe nicht in die Migration übernommen. Sie können der neuen Web-ACL verwaltete Regelgruppen hinzufügen. Die Informationen zu verwalteten Regelgruppen, einschließlich der Liste der AWS verwalteten Regeln, die in der neuen Version von verfügbar sind AWS WAF, finden Sie unter [Verwaltete Regelgruppen](#). Gehen Sie wie folgt vor, um eine verwaltete Regelgruppe hinzuzufügen:
 - a. Wählen Sie auf der Seite mit den Web-ACL-Einstellungen die Web-ACL-Registerkarte Rules (Regeln) aus.

- b. Wählen Sie Add rules (Regeln hinzufügen), und dann Add managed rule groups (Verwaltete Regelgruppen hinzufügen) aus.
- c. Erweitern Sie das Verzeichnis für den Lieferanten Ihrer Wahl und wählen Sie die Regelgruppen aus, die Sie hinzufügen möchten. AWS Marketplace Verkäufer müssen möglicherweise die Regelgruppen abonnieren. Weitere Informationen zur Verwendung verwalteter Regelgruppen in der Web-ACL finden Sie unter [Verwaltete Regelgruppen](#) und [Auswertung von Web-ACL-Regeln und -Regelgruppen](#).

Nachdem Sie die grundlegende Migration abgeschlossen haben, empfehlen wir Ihnen, Ihre Anforderungen zu überprüfen und zusätzliche Optionen in Betracht zu ziehen, um sicherzustellen, dass die neue Konfiguration so effizient wie möglich ist und die neuesten verfügbaren Sicherheitsoptionen verwendet. Siehe [Migrieren einer Web-ACL: Weitere Überlegungen](#).

Migrieren einer Web-ACL: Weitere Überlegungen

Überprüfen Sie Ihre neue Web-ACL und ziehen Sie die Optionen in Betracht, die Ihnen in der neuen Version zur Verfügung stehen, AWS WAF um sicherzustellen, dass die Konfiguration so effizient wie möglich ist und die neuesten verfügbaren Sicherheitsoptionen verwendet werden.

Zusätzliche AWS verwaltete Regeln

Erwägen Sie die Implementierung zusätzlicher AWS verwalteter Regeln in Ihrer Web-ACL, um den Sicherheitsstatus Ihrer Anwendung zu erhöhen. Diese sind ohne zusätzliche Kosten AWS WAF im Lieferumfang enthalten. AWS Verwaltete Regeln umfassen die folgenden Arten von Regelgruppen:

- Baseline-Regelgruppen bieten allgemeinen Schutz vor einer Vielzahl gängiger Bedrohungen, z. B. verhindern, dass bekannte fehlerhafte Eingaben in Ihre Anwendung gelangen, und den Zugriff auf Administratorseiten verhindern.
- Anwendungsfallspezifische Regelgruppen bieten inkrementellen Schutz für viele verschiedene Anwendungsfälle und Umgebungen.
- IP-Reputationslisten bieten Bedrohungsinformationen basierend auf der Quell-IP des Clients.

Weitere Informationen finden Sie unter [AWS Verwaltete Regeln für AWS WAF](#).

Regeloptimierung und -bereinigung

Überprüfen Sie Ihre alten Regeln und ziehen Sie eine Optimierung in Betracht, indem Sie sie neu schreiben oder veraltete entfernen. Wenn Sie beispielsweise in der Vergangenheit eine AWS

CloudFormation Vorlage aus dem technischen Dokument für OWASP Top 10 Web Application Vulnerabilities, Prepare for the OWASP Top 10 Web Application Vulnerabilities [Using AWS WAF und Our New White Paper](#) bereitgestellt haben, sollten Sie erwägen, diese Vorlage durch Managed Rules zu ersetzen. AWS Das in diesem Dokument enthaltene Konzept ist zwar weiterhin gültig und kann Ihnen beim Schreiben Ihrer eigenen Regeln helfen, aber die mit der Vorlage erstellten Regeln wurden weitgehend durch verwaltete Regeln ersetzt. AWS

CloudWatch Amazon-Metriken und Alarme

Überprüfen Sie Ihre CloudWatch Amazon-Metriken erneut und richten Sie bei Bedarf Alarme ein. Bei der Migration werden keine CloudWatch Alarme übernommen, und es ist möglich, dass Ihre Metrikenamen nicht Ihren Wünschen entsprechen.

Bewertung mit Ihrem Antragsteam

Arbeiten Sie mit Ihrem Anwendungsteam zusammen und überprüfen Sie Ihre Sicherheitslage. Finden Sie heraus, welche Felder häufig von der Anwendung analysiert werden, und fügen Sie Regeln hinzu, um die Eingabe entsprechend zu bereinigen. Überprüfen Sie, ob Edge-Fälle vorhanden sind, und fügen Sie Regeln hinzu, um diese Fälle abzufangen, wenn die Geschäftslogik der Anwendung diese nicht verarbeitet.

Planen der Umstellung

Planen Sie den Zeitpunkt der Umstellung mit Ihrem Anwendungsteam. Der Wechsel von der alten Web-ACL-Zuordnung zur neuen kann einige Zeit in Anspruch nehmen, bis er sich auf alle Bereiche erstreckt, in denen Ihre Ressourcen gespeichert sind. Die Übertragungszeit kann zwischen einigen Sekunden und mehreren Minuten liegen. Während dieser Zeit werden einige Anfragen von der alten Web-ACL und andere von der neuen Web-ACL verarbeitet. Ihre Ressourcen werden während der gesamten Umstellung geschützt, aber während der Umstellung stellen Sie möglicherweise Inkonsistenzen bei der Bearbeitung von Anfragen fest.

Wenn Sie bereit sind, umzuschalten, folgen Sie dem Verfahren unter [Migrieren einer Web-ACL: Umstellung](#).

Migrieren einer Web-ACL: Umstellung

Nachdem Sie Ihre neuen Web-ACL-Einstellungen verifiziert haben, können Sie diese anstelle Ihrer AWS WAF -Classic-Web-ACL verwenden.

Um mit der Verwendung Ihrer neuen AWS WAF Web-ACL zu beginnen

1. Ordnen Sie die AWS WAF Web-ACL den Ressourcen zu, die Sie schützen möchten. Folgen Sie dabei den Anweisungen unter [Zuordnen oder Aufheben der Zuordnung einer Web-ACL zu einer Ressource AWS](#). Dadurch werden die Ressourcen automatisch von der alten Web-ACL getrennt.

Die Übertragung des Switches kann einige Sekunden bis mehrere Minuten dauern. Während dieser Zeit werden einige Anfragen möglicherweise von der alten Web-ACL und andere von der neuen Web-ACL verarbeitet. Ihre Ressourcen werden während des gesamten Switches geschützt, Sie werden jedoch möglicherweise Inkonsistenzen bei der Bearbeitung von Anfragen feststellen, bis die Umstellung abgeschlossen ist.

2. Konfigurieren Sie die Protokollierung für die neue Web-ACL gemäß den Anweisungen unter [AWS WAF Web-ACL-Verkehr protokollieren](#).
3. (Optional) Wenn Ihre AWS WAF Classic-Web-ACL nicht mehr mit Ressourcen verknüpft ist, sollten Sie erwägen, sie vollständig aus AWS WAF Classic zu entfernen. Weitere Informationen finden Sie unter [Löschen einer Web-ACL](#).

AWS WAF Klassisch

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

AWS WAF Classic ist eine Firewall für Webanwendungen, mit der Sie die HTTP- und HTTPS-Anfragen überwachen können, die an eine Amazon API Gateway API, Amazon CloudFront oder einen Application Load Balancer weitergeleitet werden. AWS WAF Mit Classic können Sie auch den Zugriff auf Ihre Inhalte kontrollieren. Basierend auf von Ihnen angegebenen Bedingungen, z. B. den IP-Adressen, von denen Anfragen stammen, oder den Werten von Abfragezeichenfolgen, reagiert API Gateway CloudFront oder ein Application Load Balancer auf Anfragen entweder mit dem angeforderten Inhalt oder mit einem HTTP-403-Statuscode (Forbidden). Sie können auch so konfigurieren CloudFront , dass eine benutzerdefinierte Fehlerseite zurückgegeben wird, wenn eine Anfrage blockiert wird.

Themen

- [AWS WAF Classic einrichten](#)
- [So funktioniert AWS WAF Classic](#)
- [AWS WAF Klassische Preisgestaltung](#)
- [Erste Schritte mit AWS WAF Classic](#)
- [Erstellen und Konfigurieren einer Web-Zugriffskontrollliste \(Web-ACL\)](#)
- [Arbeiten mit AWS WAF klassischen Regelgruppen zur Verwendung mit AWS Firewall Manager](#)
- [Erste Schritte mit AWS Firewall Manager , um AWS WAF klassische Regeln zu aktivieren](#)
- [Tutorial: Erstellen einer AWS Firewall Manager-Richtlinie mit hierarchischen Regeln](#)
- [Protokollieren von Web-ACL-Traffic-Informationen](#)
- [Auflisten der durch ratenbasierte Regeln blockierten IP-Adressen](#)

- [So funktioniert AWS WAF Classic mit CloudFront Amazon-Funktionen](#)
- [Sicherheit in AWS WAF Classic](#)
- [AWS WAF Klassische Kontingente](#)

AWS WAF Classic einrichten

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

In diesem Thema werden vorbereitende Schritte beschrieben, wie z. B. das Erstellen eines Benutzerkontos, um Sie auf die Verwendung von AWS WAF Classic vorzubereiten. Diese werden Ihnen nicht in Rechnung gestellt. Ihnen werden nur die AWS Dienste in Rechnung gestellt, die Sie nutzen.

Note

Wenn Sie ein neuer Nutzer von AWS WAF Classic sind AWS WAF, folgen Sie diesen Einrichtungsschritten nicht. Folgen Sie stattdessen den Schritten für die neueste Version von AWS WAF, unter [Einrichtung](#).

Nachdem Sie diese Schritte abgeschlossen haben, finden Sie weitere Informationen [Erste Schritte mit AWS WAF Classic](#) zu den ersten Schritten mit AWS WAF Classic.

Note

AWS Shield Standard ist im Lieferumfang von AWS WAF Classic enthalten und erfordert keine zusätzliche Einrichtung. Weitere Informationen finden Sie unter [So funktionieren AWS Shield und Shield Advanced](#).

Bevor Sie AWS WAF Classic oder AWS Shield Advanced zum ersten Mal verwenden, führen Sie die Schritte in diesem Abschnitt durch.

Themen

- [Melde dich an für ein AWS-Konto](#)
- [Erstellen eines Administratorbenutzers](#)
- [Tools herunterladen](#)

Melde dich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie <https://portal.aws.amazon.com/billing/signup>.
2. Folgen Sie den Online-Anweisungen.

Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Tasten eingeben.

Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontos wird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem [Administratorbenutzer Administratorzugriff](#) zu und verwenden Sie nur den Root-Benutzer, um [Aufgaben auszuführen, die Root-Benutzerzugriff](#) erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu <https://aws.amazon.com/> auf und klicken Sie auf Mein Konto.

Erstellen eines Administratorbenutzers

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich [AWS Management Console](#) als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter [Anmelden als Root-Benutzer](#) im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

Anweisungen finden Sie unter [Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer \(Konsole\)](#) im IAM-Benutzerhandbuch.

Erstellen eines Administratorbenutzers

1. Aktivieren Sie das IAM Identity Center.

Anweisungen finden Sie unter [Aktivieren AWS IAM Identity Center](#) im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Administratorzugriff.

Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter [Benutzerzugriff mit der Standardeinstellung konfigurieren](#). AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie [im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal](#).

Tools herunterladen

Das AWS Management Console beinhaltet eine Konsole für AWS WAF Classic. Wenn Sie jedoch programmgesteuert auf AWS WAF Classic zugreifen möchten, finden Sie folgende Informationen:

- Wenn Sie die AWS WAF Classic-API aufrufen möchten, ohne sich um Details auf niedriger Ebene wie das Zusammenstellen von HTTP-Anfragen kümmern zu müssen, können Sie ein SDK verwenden. Die AWS SDKs stellen Funktionen und Datentypen bereit, die die Funktionalität von AWS WAF Classic und anderen Diensten zusammenfassen. Informationen zum Herunterladen eines AWS SDK finden Sie auf der entsprechenden Seite, die auch Voraussetzungen und Installationsanweisungen enthält:
 - [Java](#)
 - [JavaScript](#)
 - [.NET](#)
 - [Node.js](#)
 - [PHP](#)
 - [Python](#)
 - [Ruby](#)

Eine vollständige Liste der AWS SDKs finden Sie unter [Tools für Amazon Web Services](#).

- Wenn Sie eine Programmiersprache verwenden, für die AWS kein SDK bereitgestellt wird, dokumentiert die [AWS WAF API-Referenz](#) die Operationen, die AWS WAF Classic unterstützt.
- Das AWS Command Line Interface (AWS CLI) unterstützt AWS WAF Classic. Damit können Sie mehrere AWS Dienste von der Befehlszeile aus steuern und sie mithilfe von Skripten automatisieren. Weitere Informationen finden Sie unter [AWS Command Line Interface](#).
- AWS Tools for Windows PowerShell unterstützt AWS WAF Classic. Weitere Informationen finden Sie in der [AWS Tools for PowerShell -Cmdlet-Referenz](#).

So funktioniert AWS WAF Classic

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#).

Sie verwenden AWS WAF Classic, um zu steuern, wie API Gateway, Amazon CloudFront oder ein Application Load Balancer auf Webanfragen reagiert. Erstellen Sie zunächst Bedingungen, Regeln und Web-Zugriffskontrolllisten (Web-ACLs). Definieren Sie Ihre Bedingungen, kombinieren Sie diese in Regeln und kombinieren Sie die Regeln in einer Web-ACL.

Note

Sie können AWS WAF Classic auch verwenden, um Ihre Anwendungen zu schützen, die in Amazon Elastic Container Service (Amazon ECS) -Containern gehostet werden. Amazon ECS ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Docker-Containern in einem Cluster vereinfacht. Um diese Option zu verwenden, konfigurieren Sie Amazon ECS so, dass ein AWS WAF Classic-fähiger Application Load Balancer verwendet wird, um den HTTP/HTTPS-Verkehr (Layer 7) zwischen den Aufgaben in Ihrem Service weiterzuleiten und zu schützen. Weitere Informationen finden Sie unter dem Thema [Service Load Balancing](#) im Amazon Elastic Container Service Developer Guide.

Bedingungen

Bedingungen definieren die grundlegenden Merkmale, auf die AWS WAF Classic bei Webanfragen achten soll:

- Skripts sind möglicherweise bösartig. Angreifer betten Skripts ein, die Sicherheitslücken in Webanwendungen ausnutzen. Dies wird als Cross-Site-Scripting bezeichnet.
- IP-Adressen oder Adressbereiche, aus denen Anforderungen stammen.
- Land oder geografischer Standort, von dem die Anforderung stammt.
- Länge der angegebenen Teile der Anforderung, wie z. B. die Abfragezeichenfolge.
- SQL-Code, der möglicherweise bösartig ist. Angreifer, die versuchen, Daten aus Ihrer Datenbank zu extrahieren, indem sie bösartigen SQL-Code in eine Webanforderung einbetten. Dies wird als SQL Injection bezeichnet.
- Zeichenfolgen, die in der Anforderung angezeigt werden, z. B. Werte im User-Agent-Header oder Textzeichenfolgen in der Abfragezeichenfolge. Sie können auch reguläre Ausdrücke (Regex) verwenden, um diese Zeichenfolgen anzugeben.

Einige Bedingungen nehmen mehrere Werte an. Sie können z. B. bis zu 10,000 IP-Adressen oder IP-Adressbereiche in einer IP-Bedingung angeben.

Regeln

Sie kombinieren Bedingungen zu Regeln, um genau auf die Anfragen einzugehen, die Sie zulassen, blockieren oder zählen möchten. AWS WAF Classic bietet zwei Arten von Regeln:

Reguläre Regel

Reguläre Regeln verwenden nur Bedingungen für bestimmte Anforderungen. Basierend auf den jüngsten Anforderungen von einem Angreifer, die Sie ermittelt haben, können Sie beispielsweise eine Regel erstellen, die folgenden Bedingungen enthält:

- Die Anforderungen stammen von 192.0.2.44.
- Sie enthalten den Wert BadBot im User-Agent-Header.
- Sie scheinen schädlichen SQL-ähnlichen Code in die Abfragezeichenfolge einzufügen.

Wenn eine Regel mehrere Bedingungen enthält, wie in diesem Beispiel, sucht AWS WAF Classic nach Anfragen, die alle Bedingungen erfüllen — das heißt, es AND sind die Bedingungen zusammen.

Fügen Sie mindestens eine Bedingung zu einer regulären Regel hinzu. Eine reguläre Regel ohne Bedingungen kann keine Anforderungen erfüllen, sodass die Aktion der Regel (Zulassen, Zählen oder Blockieren) nie ausgelöst wird.

Ratenbasierte Regel

Ratenbasierte Regeln sind wie normale Regeln mit einem zusätzlichen Ratenlimit. Eine ratenbasierte Regel zählt die Anfragen, die von IP-Adressen kommen, die die Bedingungen der Regel erfüllen. Wenn die Anfragen von einer IP-Adresse innerhalb von fünf Minuten das Ratenlimit überschreiten, kann die Regel eine Aktion auslösen. Es kann ein oder zwei Minuten dauern, bis die Aktion ausgelöst wird.

Die Bedingungen sind für ratenbasierte Regeln optional. Wenn Sie in einer ratenbasierten Regel keine Bedingungen hinzufügen, gilt das Ratenlimit für alle IP-Adressen. Wenn Sie Bedingungen mit dem Ratenlimit kombinieren, gilt das Ratenlimit für IP-Adressen, die den Bedingungen entsprechen.

Basierend auf den jüngsten Anforderungen von einem Angreifer, die Sie ermittelt haben, können Sie beispielsweise eine ratenbasierte Regel erstellen, die die folgenden Bedingungen enthält:

- Die Anforderungen stammen von 192.0.2.44.

- Sie enthalten den Wert `BadBot` im `User-Agent-Header`.

In diesem ratenbasierten Regel legen Sie auch ein Ratenlimit fest. Angenommen, Sie erstellen ein Ratenlimit von 1.000. Wenn Anforderungen beide vorherigen Bedingungen erfüllen und es pro 5 Minuten mehr als 1.000 Anforderungen gibt, wird die in der Web-ACL definierte Regelaktion (Blockieren oder Zählen) ausgelöst.

Anfragen, die nicht beide Bedingungen erfüllen, werden nicht auf das Ratenlimit angerechnet und sind von dieser Regel nicht betroffen.

Nehmen wir für ein weiteres Beispiel an, Sie möchten die Anforderungen auf eine bestimmte Seite Ihrer Website beschränken. Dazu können Sie einer ratenbasierten Regel die folgende Übereinstimmungsbedingung für Zeichenfolgen hinzufügen:

- Der Teil der Anforderung, nach dem gefiltert werden soll ist `URI`.
- Der Übereinstimmungstyp ist `Starts with`.
- Ein Wert, der zugeordnet werden soll ist `login`.

Außerdem geben Sie ein `RateLimit` von 1.000 an.

Indem Sie diese ratenbasierte Regel einer Web-ACL hinzufügen, können Sie die Anforderungen an Ihre Anmeldungsseite begrenzen, ohne dass der Rest Ihrer Website davon betroffen ist.

Web-ACLs

Nachdem Sie Ihre Bedingungen kombiniert haben, kombinieren Sie die Regeln in einer Web-ACL. Hier definieren Sie eine Aktion für jede Regel — Zulassen, Blockieren oder Zählen — und eine Standardaktion:

Eine Aktion für jede Regel

Wenn eine Webanforderung alle Bedingungen in einer Regel erfüllt, kann AWS WAF Classic die Anfrage entweder blockieren oder zulassen, dass die Anfrage an die API Gateway API, CloudFront Distribution oder einen Application Load Balancer weitergeleitet wird. Sie geben für jede Regel die Aktion an, die AWS WAF Classic ausführen soll.

AWS WAF Classic vergleicht eine Anfrage mit den Regeln in einer Web-ACL in der Reihenfolge, in der Sie die Regeln aufgelistet haben. AWS WAF Classic ergreift dann die Aktion, die der ersten Regel zugeordnet ist, der die Anforderung entspricht. Wenn eine

Webanforderung beispielsweise einer Regel entspricht, die Anfragen zulässt, und einer anderen Regel, die Anfragen blockiert, lässt AWS WAF Classic die Anfrage entweder zu oder blockiert sie, je nachdem, welche Regel zuerst aufgeführt ist.

Wenn Sie eine neue Regel testen möchten, bevor Sie sie verwenden, können Sie AWS WAF Classic auch so konfigurieren, dass die Anfragen gezählt werden, die alle Bedingungen der Regel erfüllen. Wie Regeln zum Zulassen oder Blockieren von Anforderungen ist eine Regel, die Anforderungen zählt, von ihrer Position in der Liste der Regeln im Web-ACL abhängig. Wenn beispielsweise eine Webanforderung einer Regel entspricht, die Anforderungen zulässt, und einer zweiten Regel, die Anforderungen zählt, und wenn die Regel, die Anforderungen zulässt, zuerst aufgeführt ist, wird die Anforderung nicht gezählt.

Eine Standardaktion

Die Standardaktion bestimmt, ob AWS WAF Classic eine Anfrage zulässt oder blockiert, die nicht allen Bedingungen in einer der Regeln in der Web-ACL entspricht. Angenommen, Sie erstellen eine Web-ACL und fügen nur die Regel hinzu, die Sie zuvor definiert haben

- Die Anforderungen stammen von 192.0.2.44.
- Sie enthalten den Wert BadBot im User-Agent-Header.
- Sie scheinen schädlichen SQL-Code in die Abfragezeichenfolge einzufügen.

Wenn eine Anfrage nicht alle drei Bedingungen der Regel erfüllt und die Standardaktion lautet ALLOW, leitet AWS WAF Classic die Anfrage an API Gateway CloudFront oder einen Application Load Balancer weiter, und der Dienst antwortet mit dem angeforderten Objekt.

Wenn Sie einer Web-ACL zwei oder mehr Regeln hinzufügen, führt AWS WAF Classic die Standardaktion nur aus, wenn eine Anfrage nicht alle Bedingungen in einer der Regeln erfüllt. Angenommen, Sie haben eine zweite Regel mit einer Bedingung hinzugefügt.

- Anforderungen mit dem Wert BIGBadBot im User-Agent-Header.

AWS WAF Classic führt die Standardaktion nur aus, wenn eine Anfrage nicht alle drei Bedingungen in der ersten Regel und die eine Bedingung in der zweiten Regel nicht erfüllt.

In einigen Fällen kann ein interner Fehler AWS WAF auftreten, der die Antwort an Amazon API Gateway, Amazon CloudFront oder einen Application Load Balancer bezüglich der Frage, ob eine Anfrage zugelassen oder blockiert werden soll, verzögert. In diesen Fällen CloudFront wird die Anfrage in der Regel zugelassen oder der Inhalt bereitgestellt. Ein API-Gateway und Application Load Balancer lehnen die Anforderung in der Regel ab und stellen keine Inhalte bereit.

AWS WAF Klassische Preisgestaltung

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#).

Mit AWS WAF Classic zahlen Sie nur für die Web-ACLs und Regeln, die Sie erstellen, und für die Anzahl der HTTP-Anfragen, die AWS WAF Classic überprüft. Weitere Informationen finden Sie unter [AWS WAF Klassische Preisgestaltung](#).

Erste Schritte mit AWS WAF Classic

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#).

Dieses Tutorial zeigt, wie Sie AWS WAF Classic verwenden, um die folgenden Aufgaben auszuführen:

- Richten Sie AWS WAF Classic ein.
- Erstellen Sie mit der AWS WAF Classic-Konsole eine Web-Zugriffskontrollliste (Web-ACL) und geben Sie die Bedingungen an, die Sie zum Filtern von Webanfragen verwenden möchten. Sie können beispielsweise die IP-Adressen angeben, von denen die Anforderungen stammen, und die Werte in den Anforderungen, die nur von Angreifern verwendet werden.

- Fügen Sie die Bedingungen einer Regel hinzu. Regeln können Sie auf die Webanforderungen anwenden, die Sie blockieren oder zulassen möchten. Eine Webanforderung muss alle Bedingungen in einer Regel erfüllen, bevor AWS WAF Classic Anfragen auf der Grundlage der von Ihnen angegebenen Bedingungen blockiert oder zulässt.
- Fügen Sie die Regeln einer Web-ACL hinzu. Hier geben Sie an, ob Sie Webanforderungen basierend auf den Bedingungen, die Sie jeder Regel hinzufügen, blockieren oder zulassen möchten.
- Geben Sie standardmäßig entweder „Blockieren“ oder „Zulassen“ an. Dies ist die Aktion, die AWS WAF Classic ergreift, wenn eine Webanforderung keiner Ihrer Regeln entspricht.
- Wählen Sie die CloudFront Amazon-Distribution aus, für die AWS WAF Classic Webanfragen prüfen soll. Dieses Tutorial behandelt nur die Schritte für CloudFront, aber der Prozess für einen Application Load Balancer und Amazon API Gateway Gateway-APIs ist im Wesentlichen derselbe. AWS WAF Classic for CloudFront ist für alle AWS-Regionen verfügbar. AWS WAF Classic zur Verwendung mit API Gateway oder einem Application Load Balancer ist in den Regionen verfügbar, die an den [AWS Service-Endpunkten](#) aufgeführt sind.

Note

AWS In der Regel werden Ihnen weniger als 0,25 USD pro Tag für die Ressourcen in Rechnung gestellt, die Sie in diesem Tutorial erstellen. Wenn Sie das Tutorial beendet haben, empfehlen wir, dass Sie die Ressourcen löschen, um unnötige Kosten zu vermeiden.

Themen

- [Schritt 1: Classic einrichten AWS WAF](#)
- [Schritt 2: Erstellen einer Web-ACL](#)
- [Schritt 3: Erstellen einer IP-Übereinstimmungsbedingung](#)
- [Schritt 4: Erstellen einer Geo-Übereinstimmungsbedingung](#)
- [Schritt 5: Erstellen einer Zeichenfolgen-Übereinstimmungsbedingung](#)
- [Schritt 5A: Erstellen einer Regex-Bedingung \(optional\)](#)
- [Schritt 6: Erstellen einer SQL Injection-Übereinstimmungsbedingung](#)
- [Schritt 7: \(Optional\) Erstellen von zusätzlichen Bedingungen](#)
- [Schritt 8: Erstellen einer Regel und Hinzufügen von Bedingungen](#)
- [Schritt 9: Hinzufügen der Regel zu einer Web-ACL](#)

- [Schritt 10: Bereinigen Ihrer Ressourcen](#)

Schritt 1: Classic einrichten AWS WAF

Wenn Sie die allgemeinen Einrichtungsschritte unter noch nicht befolgt haben [AWS WAF Classic einrichten](#), tun Sie dies jetzt.

Schritt 2: Erstellen einer Web-ACL

Die AWS WAF Classic-Konsole führt Sie durch den Prozess der Konfiguration von AWS WAF Classic, um Webanfragen auf der Grundlage von von Ihnen festgelegter Bedingungen zu blockieren oder zuzulassen, wie z. B. die IP-Adressen, von denen die Anfragen stammen, oder die Werte in den Anfragen. In diesem Schritt erstellen Sie eine Web-ACL.

So erstellen Sie eine Web-ACL


1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wenn Sie AWS WAF Classic zum ersten Mal verwenden, wählen Sie Go to AWS WAF Classic und dann Configure web ACL aus.


Wenn Sie AWS WAF Classic schon einmal verwendet haben, wählen Sie im Navigationsbereich Web-ACLs und dann Web-ACL erstellen aus.

3. Geben Sie auf der Seite Name web ACL (Web-ACL benennen) für Web ACL name (Web-ACL-Name) einen Namen ein.

 Note

Sie können den Namen nach dem Erstellen der Web-ACL nicht mehr ändern.

4. Geben Sie als CloudWatch Metrikname einen Namen ein. Der Name darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) enthalten. Es darf keine Leerzeichen enthalten.


 Note

Sie können den Namen nach dem Erstellen der Web-ACL nicht mehr ändern.

5. Wählen Sie unter -Region eine Region aus. Wenn Sie diese Web-ACL einer CloudFront Distribution zuordnen möchten, wählen Sie Global (CloudFront).
6. Wählen Sie für AWS resource to associate die Ressource aus, die Sie mit der Web-ACL verknüpfen möchten, und dann Next.

Schritt 3: Erstellen einer IP-Übereinstimmungsbedingung

Eine IP-Übereinstimmungsbedingung gibt die IP-Adressen oder IP-Adressbereiche an, aus denen die Webanforderungen stammen. In diesem Schritt erstellen Sie eine IP-Übereinstimmungsbedingung. In einem späteren Schritt geben Sie an, ob Sie Anforderungen zulassen oder Anforderungen, die von angegebenen IP-Adressen stammen, blockieren möchten.

 Note

Weitere Informationen zu IP-Übereinstimmungsbedingungen finden Sie unter [Arbeiten mit IP-Übereinstimmungsbedingungen](#).

So erstellen Sie eine IP-Übereinstimmungsbedingung

1. Wählen Sie auf der Seite Create conditions für IP match conditions die Option Create condition.
2. Geben Sie im Dialogfeld Create IP match condition (IP-Übereinstimmungsbedingung erstellen) für Name einen Namen ein. Der Name darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) oder die folgenden Sonderzeichen enthalten: `_! "# +*},./`.
3. Geben Sie für Address (Adresse) `192.0.2.0/24` ein. Dieser in der CIDR-Notation angegebene IP-Adressbereich umfasst die IP-Adressen von `192.0.2.0` bis `192.0.2.255`. (Der IP-Adressbereich `192.0.2.0/24` ist für Beispiele reserviert, daher stammen von diesen IP-Adressen keine Anforderungen.)

AWS WAF Classic unterstützt IPv4-Adressbereiche: `/8` und jeden Bereich zwischen `/16` und `/32`.

AWS WAF Classic unterstützt die IPv6-Adressbereiche: `/24`, `/32`, `/48`, `/56`, `/64` und `/128`. (Um eine

einzelne IP-Adresse wie 192.0.2.44 anzugeben, geben Sie 192.0.2.44/32 ein.) Andere Bereiche werden nicht unterstützt.

Weitere Informationen zu CIDR-Notationen finden Sie im Wikipedia-Artikel [Classless Inter-Domain Routing](#).

4. Wählen Sie Erstellen.

Schritt 4: Erstellen einer Geo-Übereinstimmungsbedingung

Eine Geo-Übereinstimmungsbedingung gibt das Land oder die Länder an, von denen die Anforderung stammt. In diesem Schritt erstellen Sie eine Geo-Übereinstimmungsbedingung. In einem späteren Schritt geben Sie an, ob Sie Anforderungen zulassen oder Anforderungen, die von angegebenen IP-Adressen stammen, blockieren möchten, die aus den angegebenen Ländern stammen.

Note

Weitere Informationen zu Geo-Übereinstimmungsbedingungen finden Sie unter [Arbeiten mit Geo-Übereinstimmungsbedingungen](#).

So erstellen Sie eine Geo-Übereinstimmungsbedingung

1. Wählen Sie auf der Seite Create conditions für Geo match conditions die Option Create condition.
2. Geben Sie im Dialogfeld Create geo match condition (Geomatchbedingung erstellen) für Name einen Namen ein. Der Name darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) oder die folgenden Sonderzeichen enthalten: _! "# +*},./ .
3. Wählen Sie einen Standorttyp und ein Land. Derzeit kann der Location type (Standorttyp) nur Country (Land) sein.
4. Wählen Sie Add location.
5. Wählen Sie Erstellen.

Schritt 5: Erstellen einer Zeichenfolgen-Übereinstimmungsbedingung

Eine Bedingung für die Übereinstimmung mit einer Zeichenfolge identifiziert die Zeichenfolgen, nach denen AWS WAF Classic in einer Anforderung suchen soll, z. B. ein bestimmter Wert in einer Kopfzeile oder in einer Abfragezeichenfolge. Eine Zeichenfolge besteht aus druckbaren ASCII-Zeichen, aber Sie können beliebige Zeichen aus dem hexadezimalen Bereich von 0x00 bis 0xFF (dezimal 0 bis 255) angeben. In diesem Schritt erstellen Sie eine Zeichenfolgen-Übereinstimmungsbedingung. In einem späteren Schritt geben Sie an, ob Anforderungen, die die angegebenen Zeichenfolgen enthalten, zugelassen oder blockiert werden sollen.

Note

Weitere Informationen zu Zeichenfolgen-Übereinstimmungsbedingungen finden Sie unter [Arbeiten mit Zeichenfolgen-Übereinstimmungsbedingungen](#).

So erstellen Sie eine Zeichenfolgen-Übereinstimmungsbedingung

1. Wählen Sie auf der Seite Create conditions (Bedingungen erstellen) für String and regex match conditions (Zeichenfolgen- und Regex-Übereinstimmungsbedingungen) die Option Create condition (Bedingung erstellen).
2. Geben Sie im Dialogfenster Create string match condition (Zeichenfolgen-Übereinstimmungsbedingung erstellen) die folgenden Werte ein:

Name

Geben Sie einen Namen ein. Der Name darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) oder die folgenden Sonderzeichen enthalten: `_! "# ` + * } , . /`.

Typ

Wählen Sie String match.

Teil der Anforderung, nach dem gefiltert werden soll

Wählen Sie den Teil der Webanforderung aus, den AWS WAF Classic nach einer bestimmten Zeichenfolge durchsuchen soll.

Wählen Sie für dieses Beispiel Header aus.

Note

Wenn Sie für den Wert Teil der Anforderung, nach dem gefiltert werden soll, Body wählen, untersucht AWS WAF Classic nur die ersten 8192 Byte (8 KB), da nur die ersten 8192 Byte CloudFront zur Überprüfung weitergeleitet werden. Um Anfragen zuzulassen oder zu blockieren, deren Hauptteil länger als 8192 Byte ist, können Sie eine Größenbeschränkungsbedingung erstellen. (AWS WAF Classic ermittelt die Länge des Hauptteils aus den Anforderungsheadern.) Weitere Informationen finden Sie unter [Arbeiten mit Größenbeschränkungsbedingungen](#).

Header (Erforderlich, wenn "Header" als "Teil der Filter auf" festgelegt ist)

Da Sie Header als Teil der Anfrage ausgewählt haben, nach dem gefiltert werden soll, müssen Sie angeben, welchen Header AWS WAF Classic untersuchen soll. Geben Sie User-Agent ein. Bei diesem Wert wird nicht zwischen Groß- und Kleinschreibung unterschieden.

Übereinstimmungstyp

Wählen Sie aus, wo die angegebene Zeichenfolge im User-Agent-Header angezeigt werden soll, z. B. am Anfang, am Ende oder an einer beliebigen Stelle in der Zeichenfolge.

Wählen Sie in diesem Beispiel Exactly matches aus, was bedeutet, dass AWS WAF Classic Webanfragen auf einen Header-Wert überprüft, der mit dem von Ihnen angegebenen Wert identisch ist.

Transformation

Um AWS WAF Classic zu umgehen, verwenden Angreifer ungewöhnliche Formatierungen in Webanfragen, indem sie beispielsweise Leerzeichen hinzufügen oder die Anfrage ganz oder teilweise URL-kodieren. Transformationen konvertieren die Webanfrage in ein standardisierteres Format, indem sie Leerzeichen entfernen, die Anfrage per URL-Dekodierung bearbeiten oder andere Operationen ausführen, die einen Großteil der ungewöhnlichen Formatierung der Angreifer beseitigen.

Sie können nur einen einzigen Texttransformationstyp angeben.

Wählen Sie für dieses Beispiel Keiner aus.

Der Wert ist base64-kodiert

Wenn Ihr Wert in Value to match (Übereinstimmungswert) übereinstimmt bereits base64-codiert ist, aktivieren Sie dieses Kontrollkästchen.

Für dieses Beispiel aktivieren Sie das Kontrollkästchen nicht.

Wert, der zugeordnet werden soll

Geben Sie den Wert an, nach dem AWS WAF Classic in dem Teil der Webanfragen suchen soll, den Sie unter Teil der Anfrage, nach dem gefiltert werden soll, angegeben haben.

Geben Sie für dieses Beispiel ein BadBot. AWS WAF Classic untersucht den User-Agent Header in Webanfragen auf den Wert BadBot.

Die maximale Länge von Value to match ist 50 Zeichen. Wenn Sie einen base64-kodierten Wert angeben möchten, können Sie bis zu 50 Zeichen vor der Kodierung angeben.


3. Wenn Sie möchten, dass AWS WAF Classic Webanfragen auf mehrere Werte untersucht, z. B. auf einen User-Agent Header, der enthält, BadBot und auf eine Abfragezeichenfolge, die BadParameter Folgendes enthält, haben Sie zwei Möglichkeiten:
 - Wenn Sie Webanforderungen nur zulassen oder blockieren möchten, wenn diese beide Werte enthalten (AND), erstellen Sie eine Zeichenfolgen-Übereinstimmungsbedingung für jeden Wert.
 - Wenn Sie Webanforderungen, die entweder einen oder beide Werte (OR) enthalten, zulassen oder blockieren möchten, fügen Sie beide Werte derselben Zeichenfolgen-Übereinstimmungsbedingung hinzu.

Wählen Sie für dieses Beispiel Erstellen aus.

Schritt 5A: Erstellen einer Regex-Bedingung (optional)

Eine Bedingung für reguläre Ausdrücke ist eine Art von Bedingung für die Übereinstimmung mit Zeichenketten. Sie ist insofern ähnlich, als sie die Zeichenketten identifiziert, nach denen AWS WAF Classic in einer Anforderung suchen soll, z. B. einen bestimmten Wert in einer Kopfzeile oder in einer Abfragezeichenfolge. Der Hauptunterschied besteht darin, dass Sie einen regulären Ausdruck (Regex) verwenden, um das Zeichenkettenmuster anzugeben, nach dem AWS WAF Classic suchen soll. In diesem Schritt erstellen Sie eine Regex-Übereinstimmungsbedingung. In einem späteren

Schritt geben Sie an, ob Anforderungen, die die angegebenen Zeichenfolgen enthalten, zugelassen oder blockiert werden sollen.

 Note

Weitere Informationen zu Regex-Übereinstimmungsbedingungen finden Sie unter [Arbeiten mit Regex-Übereinstimmungsbedingungen](#).

So erstellen Sie eine Regex-Übereinstimmungsbedingung

1. Wählen Sie auf der Seite Create conditions (Bedingungen erstellen) für String match conditions (Zeichenfolgen-Übereinstimmungsbedingungen) die Option Create condition (Bedingung erstellen).
2. Geben Sie im Dialogfenster Create string match condition (Zeichenfolgen-Übereinstimmungsbedingung erstellen) die folgenden Werte ein:

Name

Geben Sie einen Namen ein. Der Name darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) oder die folgenden Sonderzeichen enthalten: `_!"#`+*},./`.


Typ

Wählen Sie Regex match

Teil der Anforderung, nach dem gefiltert werden soll

Wählen Sie den Teil der Webanforderung aus, den AWS WAF Classic nach einer bestimmten Zeichenfolge durchsuchen soll.

Wählen Sie für dieses Beispiel Body aus.

 Note

Wenn Sie für den Wert Teil der Anforderung, nach dem gefiltert werden soll, Body wählen, untersucht AWS WAF Classic nur die ersten 8192 Byte (8 KB), da nur die ersten 8192 Byte CloudFront zur Überprüfung weitergeleitet werden. Um Anfragen zuzulassen oder zu blockieren, deren Hauptteil länger als 8192 Byte ist, können Sie eine Größenbeschränkungsbedingung erstellen. (AWS WAF Classic ermittelt die

Länge des Hauptteils aus den Anforderungsheadern.) Weitere Informationen finden Sie unter [Arbeiten mit Größenbeschränkungsbedingungen](#).

Transformation

Um AWS WAF Classic zu umgehen, verwenden Angreifer ungewöhnliche Formatierungen in Webanfragen, indem sie beispielsweise Leerzeichen hinzufügen oder die Anfrage ganz oder teilweise URL-kodieren. Transformationen konvertieren die Webanfrage in ein standardisierteres Format, indem sie Leerzeichen entfernen, die Anfrage per URL-Dekodierung bearbeiten oder andere Operationen ausführen, die einen Großteil der ungewöhnlichen Formatierung der Angreifer beseitigen.

Sie können nur einen einzigen Texttransformationstyp angeben.

Wählen Sie für dieses Beispiel Keiner aus.

Regex-Muster zur Übereinstimmung mit der Anfrage

Wählen Sie Create regex pattern set.

Neuer Mustersatzname

Geben Sie einen Namen ein und geben Sie dann das Regex-Muster an, nach dem AWS WAF Classic suchen soll.

Geben Sie als Nächstes den regulären Ausdruck `I [a@] mAb [a@] dRequest` ein. AWS WAF Classic untersucht den User-Agent Header in Webanfragen auf die folgenden Werte:

- Ich bin BadRequest
- IamAB@dRequest
- Ich @mA BadRequest
- I@mAB@dRequest


3. Wählen Sie Create pattern set and add filter.

4. Wählen Sie Erstellen.

Schritt 6: Erstellen einer SQL Injection-Übereinstimmungsbedingung

Eine SQL-Injection-Match-Bedingung identifiziert den Teil von Webanfragen, wie z. B. einen Header oder eine Abfragezeichenfolge, den AWS WAF Classic auf böartigen SQL-Code untersuchen soll.

Angreifer nutzen SQL-Abfragen zum Extrahieren von Daten aus Ihrer Datenbank. In diesem Schritt erstellen Sie eine SQL Injections-Übereinstimmungsbedingung. In einem späteren Schritt geben Sie an, ob Sie Anforderungen zulassen oder blockieren möchten, die möglicherweise schädlichen SQL-Code enthalten.

 Note

Weitere Informationen zu Zeichenfolgen-Übereinstimmungsbedingungen finden Sie unter [Arbeiten mit SQL Injections-Übereinstimmungsbedingungen](#).

So erstellen Sie eine SQL Injections-Übereinstimmungsbedingung

1. Wählen Sie auf der Seite Create conditions für SQL injection match conditions die Option Create condition.
2. Geben Sie im Dialogfenster Create SQL injection match condition (SQL-Injection-Übereinstimmungsbedingungen erstellen) die folgenden Werte ein:


Name

Geben Sie einen Namen ein.

Teil der Anforderung, nach dem gefiltert werden soll

Wählen Sie den Teil der Webanfragen aus, den AWS WAF Classic auf böartigen SQL-Code untersuchen soll.

Wählen Sie für dieses Beispiel Query string.

 Note

Wenn Sie für den Wert Teil der Anforderung, nach dem gefiltert werden soll, Body wählen, untersucht AWS WAF Classic nur die ersten 8192 Byte (8 KB), da nur die ersten 8192 Byte CloudFront zur Überprüfung weitergeleitet werden. Um Anfragen zuzulassen oder zu blockieren, deren Hauptteil länger als 8192 Byte ist, können Sie eine Größenbeschränkungsbedingung erstellen. (AWS WAF Classic ermittelt die Länge des Hauptteils aus den Anforderungsheadern.) Weitere Informationen finden Sie unter [Arbeiten mit Größenbeschränkungsbedingungen](#).

Transformation

Wählen Sie für dieses Beispiel URL decode aus.

Angreifer verwenden ungewöhnliche Formatierungen, wie z. B. die URL-Kodierung, um AWS WAF Classic zu umgehen. Mit der URL-Dekodierungsoption wird ein Teil dieser Formatierung in der Webanforderung entfernt, bevor AWS WAF Classic die Anfrage überprüft.

Sie können nur einen einzigen Texttransformationstyp angeben.

3. Wählen Sie Erstellen.
4. Wählen Sie Weiter aus.

Schritt 7: (Optional) Erstellen von zusätzlichen Bedingungen


AWS WAF Classic beinhaltet weitere Bedingungen, darunter die folgenden:

- Bedingungen für Größenbeschränkungen — Identifiziert den Teil von Webanfragen, z. B. einen Header oder eine Abfragezeichenfolge, dessen Länge AWS WAF Classic überprüfen soll. Weitere Informationen finden Sie unter [Arbeiten mit Größenbeschränkungsbedingungen](#).
- Siteübergreifende Scripting-Abgleichsbedingungen — Identifiziert den Teil der Webanfragen, wie z. B. eine Kopfzeile oder eine Abfragezeichenfolge, den Sie auf schädliche Skripts untersuchen AWS WAF möchten. Weitere Informationen finden Sie unter [Arbeiten mit Cross-Site-Scripting-Übereinstimmungsbedingungen](#).

Sie können diese Bedingungen jetzt erstellen oder zum Schritt [Schritt 8: Erstellen einer Regel und Hinzufügen von Bedingungen](#) wechseln.

Schritt 8: Erstellen einer Regel und Hinzufügen von Bedingungen

Sie erstellen eine Regel, um die Bedingungen anzugeben, nach denen AWS WAF Classic in Webanfragen suchen soll. Wenn Sie einer Regel mehr als eine Bedingung hinzufügen, muss eine Webanforderung allen Bedingungen in der Regel entsprechen, damit AWS WAF Classic Anfragen, die auf dieser Regel basieren, zulässt oder blockiert.

 Note

Weitere Informationen zu Regeln finden Sie unter [Arbeiten mit Regeln](#).

So erstellen Sie eine Regel und fügen Bedingungen hinzu

1. Wählen Sie auf der Seite Create rules die Option Create rule.
2. Geben Sie im Dialogfenster Create rule (Regel erstellen) die folgenden Werte ein:

Name

Geben Sie einen Namen ein.

CloudWatch Name der Metrik

Geben Sie einen Namen für die CloudWatch Metrik ein, die AWS WAF Classic erstellen und der Regel zuordnen wird. Der Name darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) enthalten. Es darf keine Leerzeichen enthalten.

Regeltyp

Wählen Sie entweder Regular rule (Reguläre Regel) oder Rate-based rule (Ratenbasierte Regel). Ratenbasierte Regeln sind identisch mit regulären Regeln, berücksichtigen aber auch, wie viele Anfragen von der identifizierten IP-Adresse in einem Zeitraum von fünf Minuten eingehen. Weitere Informationen zu den Regelarten finden Sie unter [So funktioniert AWS WAF Classic](#). Wählen Sie für dieses Beispiel Regular rule aus.

Ratenlimit

Geben Sie bei einer ratenbasierten Regel die maximale Anzahl von Anfragen ein, die in einem Zeitraum von fünf Minuten von einer IP-Adresse, die den Bedingungen der Regel entspricht, zulässig sind.

3. Für die erste Bedingung, die Sie der Regel hinzufügen möchten, legen Sie die folgenden Einstellungen fest:
 - Wählen Sie aus, ob AWS WAF Classic Anfragen zulassen oder blockieren soll, je nachdem, ob eine Webanforderung den Einstellungen in der Bedingung entspricht oder nicht.

Wählen Sie für dieses Beispiel `does` aus.

- Wählen Sie die Art der Bedingung aus, die Sie der Regel hinzufügen möchten, also eine IP-Übereinstimmungsbedingungen, eine Zeichenfolgen-Übereinstimmungsbedingung oder eine SQL Injections-Übereinstimmungsbedingung.

Wählen Sie für dieses Beispiel originate from IP addresses in aus.

- Wählen Sie die Bedingung aus, die Sie der Regel hinzufügen möchten.

Wählen Sie für dieses Beispiel die IP-Übereinstimmungsbedingung aus, die Sie in vorherigen Aufgaben erstellt haben.

4. Klicken Sie auf Bedingung hinzufügen.
5. Fügen Sie die Geo-Übereinstimmungsbedingung hinzu, die Sie zuvor erstellt haben. Geben Sie die folgenden Werte an:
 - Wenn eine Anfrage
 - stammt aus einem geografischen Standort in
 - Wählen Sie die Geo-Übereinstimmungsbedingung aus.
6. Wählen Sie Add another condition (Eine weitere Bedingung hinzufügen) aus.
7. Fügen Sie die Zeichenfolgen-Übereinstimmungsbedingung hinzu, die Sie zuvor erstellt haben. Geben Sie die folgenden Werte an:
 - Wenn eine Anfrage
 - mindestens einem der Filter in der Zeichenfolgen-Übereinstimmungsbedingung entspricht
 - Wählen Sie die Zeichenfolgen-Übereinstimmungsbedingung aus.
8. Klicken Sie auf Bedingung hinzufügen.
9. Fügen Sie die SQL Injections-Übereinstimmungsbedingung hinzu, die Sie zuvor erstellt haben. Geben Sie die folgenden Werte an:
 - Wenn eine Anfrage
 - mindestens einem der Filter in der SQL Injections-Übereinstimmungsbedingung entspricht
 - Wählen Sie die SQL Injections-Übereinstimmungsbedingung aus.
10. Klicken Sie auf Bedingung hinzufügen.
11. Fügen Sie die Größenbeschränkungsbedingung hinzu, die Sie zuvor erstellt haben. Geben Sie die folgenden Werte an:
 - Wenn eine Anfrage

- mindestens einem der Filter in der Größenbeschränkungsbedingung entspricht
 - Wählen Sie die Größenbeschränkungsbedingung aus.
12. Wenn Sie andere Bedingungen erstellt haben, z. B. eine Regex-Bedingung, fügen Sie sie auf ähnliche Weise hinzu.
 13. Wählen Sie Erstellen.
 14. Wählen Sie für die Default action Allow all requests that don't match any rules.
 15. Wählen Sie Review and create.

Schritt 9: Hinzufügen der Regel zu einer Web-ACL

Wenn Sie die Regel zu Web-ACL hinzufügen, können Sie die folgenden Einstellungen vornehmen:

- Die Aktion, die AWS WAF Classic bei Webanfragen ausführen soll, die alle Bedingungen der Regel erfüllen: Anfragen zulassen, blockieren oder zählen.
- Die Standardaktion für die Web-ACL. Dies ist die Aktion, die AWS WAF Classic bei Webanfragen ausführen soll, die nicht alle Bedingungen der Regel erfüllen: Anfragen zulassen oder blockieren.

AWS WAF Classic beginnt damit, CloudFront Webanfragen zu blockieren, die alle folgenden Bedingungen erfüllen (und alle anderen, die Sie möglicherweise hinzugefügt haben):


- Der Wert des User-Agent-Headers ist BadBot
- Wenn Sie die Regex-Bedingung erstellt und hinzugefügt haben) Der Wert von Body ist eine der vier Zeichenfolgen, die dem Muster `I[a@mAB[a]dRequest` entsprechen
- Die Anforderungen stammen von IP-Adressen im Bereich 192.0.2.0-192.0.2.255
- Die Anfragen stammen aus dem Land, das Sie in Ihrer Geomatch-Bedingung ausgewählt haben.
- Sie scheinen schädlichen SQL-Code in die Abfragezeichenfolge einzufügen.

AWS WAF Classic ermöglicht es CloudFront, auf Anfragen zu antworten, die nicht alle drei dieser Bedingungen erfüllen.

Schritt 10: Bereinigen Ihrer Ressourcen

Sie haben das Tutorial jetzt erfolgreich abgeschlossen. Um zu verhindern, dass für Ihr Konto zusätzliche AWS WAF Classic-Gebühren anfallen, sollten Sie die von Ihnen erstellten AWS

WAF Classic-Objekte bereinigen. Alternativ können Sie die Konfiguration so ändern, dass sie die Anforderungen erfüllt, die Sie tatsächlich zulassen, blockieren und zählen möchten.

 Note

AWS berechnet Ihnen in der Regel weniger als 0,25 USD pro Tag für die Ressourcen, die Sie in diesem Tutorial erstellen. Wenn Sie fertig sind, empfehlen wir, dass Sie die Ressourcen löschen, um unnötige Kosten zu vermeiden.

Um die Objekte zu löschen, für die AWS WAF Classic Gebühren erhebt

1. Trennen Sie Ihre Web-ACL von Ihrer CloudFront Distribution:
 - a. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.
 - b. Wählen Sie den Namen der Web-ACL aus, die Sie löschen möchten. Dadurch wird im rechten Bereich eine Seite mit den Details der Web-ACL geöffnet.
 - c. Gehen Sie im rechten Bereich auf der Registerkarte Regeln zum Abschnitt AWS Ressourcen, die diese Web-ACL verwenden. Wählen Sie für die CloudFront Distribution, der Sie die Web-ACL zugeordnet haben, das X in der Spalte Typ aus.
2. Entfernen Sie die Bedingungen Ihrer Regel:
 - a. Wählen Sie im Navigationsbereich Regeln aus.
 - b. Wählen Sie die Regel aus, die Sie während des Tutorials erstellt haben.
 - c. Wählen Sie Edit rule.
 - d. Wählen Sie x rechts neben jeder Bedingung aus.
 - e. Wählen Sie Aktualisieren.
3. Entfernen Sie die Regel aus Ihrer Web-ACL und löschen Sie die Web-ACL:
 - a. Wählen Sie im Navigationsbereich Web ACLs aus.
 - b. Wählen Sie den Namen der Web-ACL, die Sie während des Tutorials erstellt haben. Dadurch wird im rechten Bereich eine Seite mit den Details der Web-ACL geöffnet.
 - c. Wählen Sie auf der Registerkarte Rules die Option Edit web ACL.

- d. Wählen Sie x rechts neben der Regel aus.
 - e. Wählen Sie Actions und anschließend Delete web ACL (Web-ACL löschen).
4. Löschen Sie die Regel:
- a. Wählen Sie im Navigationsbereich Regeln aus.
 - b. Wählen Sie die Regel aus, die Sie während des Tutorials erstellt haben.
 - c. Wählen Sie Löschen aus.
 - d. Wählen Sie im Dialogfeld Löschen zur Bestätigung erneut Löschen aus.

AWS WAF Classic berechnet keine Gebühren für Bedingungen. Wenn Sie die Bereinigung jedoch abschließen möchten, gehen Sie wie folgt vor, um Filter aus Bedingungen zu entfernen und die Bedingungen zu löschen.

So löschen Sie Filter und Bedingungen

1. Löschen Sie erst den IP-Adressbereich in Ihrer IP-Übereinstimmungsbedingung und dann die IP-Übereinstimmungsbedingung:
 - a. Wählen Sie im Navigationsbereich der AWS WAF Classic-Konsole IP-Adressen aus.
 - b. Wählen Sie die IP-Übereinstimmungsbedingung aus, die Sie während des Tutorials erstellt haben.
 - c. Aktivieren Sie das Kontrollkästchen für den IP-Adressbereich, den Sie hinzugefügt haben.
 - d. Wählen Sie Delete IP address or range.
 - e. Wählen Sie im Bereich IP match conditions die Option Löschen.
 - f. Wählen Sie im Dialogfeld Löschen zur Bestätigung erneut Löschen aus.
2. Löschen Sie erst die Filter in der SQL Injections-Übereinstimmungsbedingung und dann die SQL Injections-Übereinstimmungsbedingung selbst:
 - a. Wählen Sie im Navigationsbereich SQL injection aus.
 - b. Wählen Sie die SQL Injections-Übereinstimmungsbedingung aus, die Sie während des Tutorials erstellt haben.
 - c. Aktivieren Sie das Kontrollkästchen für den Filter, den Sie hinzugefügt haben.
 - d. Wählen Sie Delete filter.
 - e. Wählen Sie im Bereich SQL injection match conditions die Option Löschen aus.

- f. Wählen Sie im Dialogfeld Löschen zur Bestätigung erneut Löschen aus.
3. Löschen Sie erst den Filter in der Zeichenfolgen-Übereinstimmungsbedingung und dann die Zeichenfolgen-Übereinstimmungsbedingung selbst:
 - a. Wählen Sie im Navigationsbereich String and regex matching aus.
 - b. Wählen Sie die Zeichenfolgen-Übereinstimmungsbedingung aus, die Sie während des Tutorials erstellt haben.
 - c. Aktivieren Sie das Kontrollkästchen für den Filter, den Sie hinzugefügt haben.
 - d. Wählen Sie Delete filter.
 - e. Wählen Sie im Bereich String match conditions die Option Löschen.
 - f. Wählen Sie im Dialogfeld Löschen zur Bestätigung erneut Löschen aus.
4. Wenn Sie eine erstellt haben, löschen Sie den Filter in Ihrer Regex-Übereinstimmungsbedingung und löschen Sie die Regex-Übereinstimmungsbedingung:
 - a. Wählen Sie im Navigationsbereich String and regex matching aus.
 - b. Wählen Sie die Regex-Übereinstimmungsbedingung aus, die Sie während des Tutorials erstellt haben.
 - c. Aktivieren Sie das Kontrollkästchen für den Filter, den Sie hinzugefügt haben.
 - d. Wählen Sie Delete filter.
 - e. Wählen Sie im Bereich Regex match conditions die Option Delete.
 - f. Wählen Sie im Dialogfeld Löschen zur Bestätigung erneut Löschen aus.
5. Löschen Sie erst den Filter in Ihrer Größenbeschränkungsbedingung und dann die Größenbeschränkungsbedingung selbst:
 - a. Wählen Sie im Navigationsbereich Size constraints aus.
 - b. Wählen Sie die Größenbeschränkungsbedingung aus, die Sie während des Tutorials erstellt haben.
 - c. Aktivieren Sie das Kontrollkästchen für den Filter, den Sie hinzugefügt haben.
 - d. Wählen Sie Delete filter.
 - e. Wählen Sie im Bereich Size constraint conditions die Option Löschen.
 - f. Wählen Sie im Dialogfeld Löschen zur Bestätigung erneut Löschen aus.

Erstellen und Konfigurieren einer Web-Zugriffskontrollliste (Web-ACL)

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Eine Web-Zugriffskontrollliste (Web ACL) gibt Ihnen eine genaue Kontrolle über die Webanfragen, auf die Ihre Amazon API Gateway Gateway-API, CloudFront Amazon-Distribution oder Ihr Application Load Balancer reagiert. Sie können die folgenden Arten von Anforderungen zulassen oder blockieren:

- Stammen von einer IP-Adresse oder einem Bereich von IP-Adressen
- Herkunft aus einem bestimmten Land oder Ländern
- Enthält eine angegebene Zeichenfolge oder stimmt mit einem regulären Ausdruck (Regex) in einem bestimmten Teil von Anforderungen überein.
- Überschreiten eine angegebene Länge
- Enthalten möglicherweise schädlichen SQL-Code (bezeichnet als SQL Injection)
- Enthalten möglicherweise schädliche Skripts (bezeichnet als Cross-Site-Scripting)

Sie können alle Kombinationen dieser Bedingungen testen oder Webanforderungen blockieren oder zählen, die nicht nur den angegebenen Bedingungen entsprechen, sondern auch in einem 5-Minuten-Zeitraum eine angegebene Anzahl von Anforderungen überschreiten.

Um die Anforderungen auszuwählen, für die Sie den Zugriff auf Ihre Inhalte zulassen oder blockieren möchten, führen Sie die folgenden Aufgaben aus:

1. Wählen Sie eine der Standardaktionen Zulassen oder Blockieren für Webanforderungen aus, die keiner der angegebenen Bedingungen entsprechen. Weitere Informationen finden Sie unter [Bestimmen der Standardaktion für eine Web-ACL](#).

2. Geben Sie die Bedingungen an, unter denen Sie Anforderungen zulassen oder blockieren möchten:

- Um Anforderungen basierend darauf, ob sie schädliche Skripts enthalten, zuzulassen oder zu blockieren, erstellen Sie Cross-Site-Scripting-Übereinstimmungsbedingungen. Weitere Informationen finden Sie unter [Arbeiten mit Cross-Site-Scripting-Übereinstimmungsbedingungen](#).
- Um auf IP-Adressen basierende Anforderungen zuzulassen oder zu blockieren, erstellen Sie IP-Übereinstimmungsbedingungen. Weitere Informationen finden Sie unter [Arbeiten mit IP-Übereinstimmungsbedingungen](#).
- Um Anforderungen basierend auf dem Land, aus dem sie stammen, zuzulassen oder zu blockieren, erstellen Sie Geo-Übereinstimmungsbedingungen. Weitere Informationen finden Sie unter [Arbeiten mit Geo-Übereinstimmungsbedingungen](#).
- Um Anforderungen basierend darauf, ob sie eine bestimmte Länge überschreiten, zuzulassen oder zu blockieren, erstellen Sie Größenbeschränkungsbedingungen. Weitere Informationen finden Sie unter [Arbeiten mit Größenbeschränkungsbedingungen](#).
- Um Anforderungen basierend darauf, ob sie möglicherweise schädlichen SQL-Code enthalten, zuzulassen oder zu blockieren, erstellen Sie SQL Injections-Übereinstimmungsbedingungen. Weitere Informationen finden Sie unter [Arbeiten mit SQL Injections-Übereinstimmungsbedingungen](#).
- Um Anforderungen basierend auf darin enthaltenen Zeichenfolgen zuzulassen oder zu blockieren, erstellen Sie Zeichenfolgen-Übereinstimmungsbedingungen. Weitere Informationen finden Sie unter [Arbeiten mit Zeichenfolgen-Übereinstimmungsbedingungen](#).
- Um Anforderungen zuzulassen oder zu blockieren, die auf einem Regex-Muster basieren, das in den Anforderungen angezeigt wird, erstellen Sie Regex-Übereinstimmungsbedingungen. Weitere Informationen finden Sie unter [Arbeiten mit Regex-Übereinstimmungsbedingungen](#).

3. Fügen Sie die Bedingungen einer oder mehreren Regeln hinzu. Wenn Sie derselben Regel mehr als eine Bedingung hinzufügen, müssen Webanfragen alle Bedingungen erfüllen, damit AWS WAF Classic Anfragen basierend auf der Regel zulässt oder blockiert. Weitere Informationen finden Sie unter [Arbeiten mit Regeln](#). Optional können Sie anstelle einer regulären Regel eine ratenbasierte Regel verwenden, um die Anzahl der Anfragen von jeder IP-Adresse, die die Bedingungen erfüllt, zu begrenzen.

4. Fügen Sie die Regeln zu einer Web-ACL hinzu. Geben Sie für jede Regel an, ob AWS WAF Classic Anfragen basierend auf den Bedingungen, die Sie der Regel hinzugefügt haben, zulassen oder blockieren soll. Wenn Sie einer Web-ACL mehr als eine Regel hinzufügen, bewertet AWS

WAF Classic die Regeln in der Reihenfolge, in der sie in der Web-ACL aufgeführt sind. Weitere Informationen finden Sie unter [Arbeiten mit Web-ACLs](#).

Wenn Sie eine neue Regel hinzufügen oder bestehende Regeln aktualisieren, kann es bis zu einer Minute dauern, bis diese Änderungen erscheinen und in Ihren Web-ACLs und Ressourcen aktiv sind.

Themen

- [Verwenden von Bedingungen](#)
- [Arbeiten mit Regeln](#)
- [Arbeiten mit Web-ACLs](#)

Verwenden von Bedingungen

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Geben Sie die Bedingungen an, unter denen Sie Anforderungen zulassen oder blockieren möchten.

- Um Anforderungen basierend darauf, ob sie schädliche Skripts enthalten, zuzulassen oder zu blockieren, erstellen Sie Cross-Site-Scripting-Übereinstimmungsbedingungen. Weitere Informationen finden Sie unter [Arbeiten mit Cross-Site-Scripting-Übereinstimmungsbedingungen](#).
- Um auf IP-Adressen basierende Anforderungen zuzulassen oder zu blockieren, erstellen Sie IP-Übereinstimmungsbedingungen. Weitere Informationen finden Sie unter [Arbeiten mit IP-Übereinstimmungsbedingungen](#).
- Um Anforderungen basierend auf dem Land, aus dem sie stammen, zuzulassen oder zu blockieren, erstellen Sie Geo-Übereinstimmungsbedingungen. Weitere Informationen finden Sie unter [Arbeiten mit Geo-Übereinstimmungsbedingungen](#).

- Um Anforderungen basierend darauf, ob sie eine bestimmte Länge überschreiten, zuzulassen oder zu blockieren, erstellen Sie Größenbeschränkungsbedingungen. Weitere Informationen finden Sie unter [Arbeiten mit Größenbeschränkungsbedingungen](#).
- Um Anforderungen basierend darauf, ob sie möglicherweise schädlichen SQL-Code enthalten, zuzulassen oder zu blockieren, erstellen Sie SQL Injections-Übereinstimmungsbedingungen. Weitere Informationen finden Sie unter [Arbeiten mit SQL Injections-Übereinstimmungsbedingungen](#).
- Um Anforderungen basierend auf darin enthaltenen Zeichenfolgen zuzulassen oder zu blockieren, erstellen Sie Zeichenfolgen-Übereinstimmungsbedingungen. Weitere Informationen finden Sie unter [Arbeiten mit Zeichenfolgen-Übereinstimmungsbedingungen](#).
- Um Anforderungen zuzulassen oder zu blockieren, die auf einem Regex-Muster basieren, das in den Anforderungen angezeigt wird, erstellen Sie Regex-Übereinstimmungsbedingungen. Weitere Informationen finden Sie unter [Arbeiten mit Regex-Übereinstimmungsbedingungen](#).

Themen

- [Arbeiten mit Cross-Site-Scripting-Übereinstimmungsbedingungen](#)
- [Arbeiten mit IP-Übereinstimmungsbedingungen](#)
- [Arbeiten mit Geo-Übereinstimmungsbedingungen](#)
- [Arbeiten mit Größenbeschränkungsbedingungen](#)
- [Arbeiten mit SQL Injections-Übereinstimmungsbedingungen](#)
- [Arbeiten mit Zeichenfolgen-Übereinstimmungsbedingungen](#)
- [Arbeiten mit Regex-Übereinstimmungsbedingungen](#)

Arbeiten mit Cross-Site-Scripting-Übereinstimmungsbedingungen

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Angreifer fügen manchmal Skripts in Webanforderungen ein, um Schwachstellen in Webanwendungen auszunutzen. Sie können eine oder mehrere websiteübergreifende Scripting-Vergleichsbedingungen erstellen, um die Teile von Webanfragen zu identifizieren, z. B. den URI oder die Abfragezeichenfolge, die AWS WAF Classic auf mögliche bösartige Skripts untersuchen soll. Im weiteren Verlauf des Prozesses können Sie beim Erstellen einer Web-ACL angeben, ob Sie Anforderungen zulassen oder blockieren möchten, die schädliche Skripts enthalten.

Themen

- [Erstellen von Cross-Site-Scripting-Übereinstimmungsbedingungen](#)
- [Werte, die Sie beim Erstellen oder Bearbeiten von Cross-Site-Scripting-Übereinstimmungsbedingungen angeben](#)
- [Hinzufügen und Löschen von Filtern in einer Cross-Site-Scripting-Übereinstimmungsbedingung](#)
- [Löschen von Cross-Site-Scripting-Übereinstimmungsbedingungen](#)

Erstellen von Cross-Site-Scripting-Übereinstimmungsbedingungen


Beim Erstellen von Cross-Site-Scripting-Übereinstimmungsbedingungen geben Sie Filter an. Die Filter geben den Teil der Webanfragen an, den AWS WAF Classic auf schädliche Skripts untersuchen soll, z. B. den URI oder die Abfragezeichenfolge. Sie können einer Cross-Site-Scripting-Übereinstimmungsbedingung mehrere Filter hinzufügen oder eine separate Bedingung für jeden Filter erstellen. So wirkt sich jede Konfiguration auf das Verhalten von AWS WAF Classic aus:

- Mehr als ein Filter pro Cross-Site-Scripting-Übereinstimmungsbedingung (empfohlen) — Wenn Sie einer Regel eine Cross-Site-Scripting-Abgleichsbedingung hinzufügen, die mehrere Filter enthält, und die Regel einer Web-ACL hinzufügen, muss eine Webanforderung nur einem der Filter in der Cross-Site-Scripting-Abgleichsbedingung entsprechen, damit AWS WAF Classic die Anfrage auf der Grundlage dieser Bedingung zulässt oder blockiert.

Beispiel: Sie erstellen eine Cross-Site-Scripting-Übereinstimmungsbedingung, die zwei Filter enthält. Ein Filter weist AWS WAF Classic an, den URI auf schädliche Skripts zu untersuchen, und der andere weist AWS WAF Classic an, die Abfragezeichenfolge zu untersuchen. AWS WAF Classic lässt Anfragen zu oder blockiert sie, wenn sie bösartige Skripts entweder im URI oder in der Abfragezeichenfolge zu enthalten scheinen.

- Ein Filter pro Cross-Site-Scripting-Übereinstimmungsbedingung — Wenn Sie die separaten Cross-Site-Scripting-Abgleichsbedingungen zu einer Regel hinzufügen und die Regel zu einer Web-ACL hinzufügen, müssen Webanfragen alle Bedingungen erfüllen, damit AWS WAF Classic Anfragen basierend auf den Bedingungen zulassen oder blockieren kann.

Angenommen Sie erstellen zwei Bedingungen, die jeweils einen der beiden Filter im vorherigen Beispiel enthalten. Wenn Sie beide Bedingungen zu derselben Regel hinzufügen und die Regel zu einer Web-ACL hinzufügen, erlaubt oder blockiert AWS WAF Classic Anfragen nur, wenn sowohl der URI als auch die Abfragezeichenfolge schädliche Skripts zu enthalten scheinen.

 Note

Wenn Sie einer Regel eine Cross-Site-Scripting-Abgleichsbedingung hinzufügen, können Sie AWS WAF Classic auch so konfigurieren, dass Webanfragen, die keine schädlichen Skripts zu enthalten scheinen, zugelassen oder blockiert werden.

So erstellen Sie eine Cross-Site Scripting-Übereinstimmungsbedingung

1. [Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter `https://console.aws.amazon.com/wafv2/`.](https://console.aws.amazon.com/wafv2/)

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich Cross-site scripting.
3. Wählen Sie Create condition.
4. Geben Sie die entsprechenden Filtereinstellungen an. Weitere Informationen finden Sie unter [Werte, die Sie beim Erstellen oder Bearbeiten von Cross-Site-Scripting-Übereinstimmungsbedingungen angeben](#).
5. Wählen Sie Add another filter.
6. Wenn Sie einen anderen Filter hinzufügen möchten, wiederholen Sie die Schritte 4 und 5.
7. Wählen Sie danach Erstellen aus.

Werte, die Sie beim Erstellen oder Bearbeiten von Cross-Site-Scripting-Übereinstimmungsbedingungen angeben

Beim Erstellen oder Aktualisieren einer Cross-Site-Scripting-Übereinstimmungsbedingung, geben Sie die folgenden Werte an:

Name

Der Name der Cross-Site-Scripting-Übereinstimmungsbedingung.

Der Name darf nur die Zeichen A-Z, a-z, 0-9 und die folgenden Sonderzeichen enthalten: `_! "#`+*},./` . Sie können den Namen einer Bedingung nicht mehr ändern, nachdem Sie sie erstellt haben.

Teil der Anforderung, nach dem gefiltert werden soll

Wählen Sie den Teil jeder Webanfrage aus, den AWS WAF Classic auf böartige Skripts untersuchen soll:

Header

Ein angegebener Anforderungs-Header, wie z. B. der `User-Agent`- oder `Referer`-Header. Wenn Sie Header auswählen, geben Sie den Namen des Headers im Feld Header an.

HTTP-Methode

Die HTTP-Methode, die die Art des Vorgangs angibt, zu dem die Anfrage den Ursprung auffordert. CloudFront unterstützt die folgenden Methoden: `DELETE`, `GET`, `HEAD`, `OPTIONS`, `PATCH`, `POST`, und `PUT`.

Abfragezeichenfolge

Der Teil einer URL nach einem `?`-Zeichen, sofern vorhanden.

Note

Für Cross-Site-Scripting-Übereinstimmungsbedingungen empfehlen wir, dass Sie `All query parameters (values only)` (Alle Abfrageparameter (nur Werte)) anstelle von `Query string` (Abfragezeichenfolge) für `Part of the request to filter on` (Teil der Anforderung, nach dem gefiltert werden soll) auswählen.

URI

Der URI-Pfad der Anfrage, der die Ressource identifiziert, `/images/daily-ad.jpg` z. B. Dies beinhaltet nicht die Abfragezeichenfolge oder die Fragmentkomponenten der URI. Informationen dazu finden Sie unter [Uniform Resource Identifier \(URI\): Generic Syntax](#).

Sofern keine Transformation angegeben ist, ist ein URI nicht normalisiert und wird genauso geprüft, wie er im Rahmen der Anfrage vom Client AWS empfangen wird. Eine Transformation formatiert die URI wie vorgegeben neu.

Fließtext

Der Teil einer Anforderung, der zusätzliche Daten enthält, die Sie als HTTP-Anforderungstext an Ihren Webserver senden möchten, wie z. B. Formulardaten.

Note

Wenn Sie für den Wert Teil der Anforderung, nach dem gefiltert werden soll, Body wählen, untersucht AWS WAF Classic nur die ersten 8192 Byte (8 KB). Um Anfragen zuzulassen oder zu blockieren, deren Hauptteil länger als 8192 Byte ist, können Sie eine Größenbeschränkungsbedingung erstellen. (AWS WAF Classic ermittelt die Länge des Hauptteils aus den Anforderungsheadern.) Weitere Informationen finden Sie unter [Arbeiten mit Größenbeschränkungsbedingungen](#).

Einzelner Abfrageparameter (ausschließlich Wert)

Jeder Parameter, den Sie als Teil der Abfragezeichenfolge definiert haben. Wenn die URL beispielsweise „www.xyz.com? UserName =abc& SalesRegion =seattle“ lautet, können Sie entweder dem Parameter oder einen Filter hinzufügen. UserNameSalesRegion

Wenn Sie Einzelner Abfrageparameter (ausschließlich Wert) auswählen, legen Sie auch einen Abfrageparameternamen fest. Dies ist der Parameter in der Abfragezeichenfolge, den Sie überprüfen werden, z. B. oder. UserNameSalesRegion Die maximale Länge für den Abfrageparameternamen beträgt 30 Zeichen. Der Abfrageparametername berücksichtigt keine Groß- und Kleinschreibung. Wenn Sie beispielsweise den Namen des Query-Parameters angeben UserName, entspricht dies allen Varianten von UserName, z. B. UsERName und userName.

Alle Abfrageparameter (ausschließlich Werte)

Ähnlich wie Einzelner Abfrageparameter (nur Wert), untersucht AWS WAF Classic jedoch nicht die Werte eines einzelnen Parameters, sondern alle Parameterwerte innerhalb der Abfragezeichenfolge auf mögliche bösartige Skripts. Wenn die URL beispielsweise „www.xyz.com? UserName =abc& SalesRegion =seattle“ lautet und Sie Alle Abfrageparameter (nur Werte) auswählen, löst AWS WAF Classic eine Übereinstimmung

aus, wenn es sich entweder um den Wert von oder um mögliche bösartige Skripts handelt.

UserNameSalesRegion

Header

Wenn Sie Header für Teil der Anfrage, nach der gefiltert werden soll, ausgewählt haben, wählen Sie einen Header aus der Liste der allgemeinen Header aus, oder geben Sie den Namen eines Headers ein, den Classic auf bösartige Skripts untersuchen soll. AWS WAF

Transformation

Eine Transformation formatiert eine Webanforderung neu, bevor AWS WAF Classic die Anfrage überprüft. Dadurch werden einige der ungewöhnlichen Formatierungen vermieden, die Angreifer in Webanfragen verwenden, um Classic zu umgehen AWS WAF .

Sie können nur einen einzigen Texttransformationstyp angeben.

Transformationen können die folgenden Vorgänge ausführen:

None

AWS WAF Classic führt keine Texttransformationen an der Webanforderung durch, bevor überprüft wird, ob die Zeichenfolge in Value übereinstimmt.

In Kleinbuchstaben konvertieren

AWS WAF Classic konvertiert Großbuchstaben (A-Z) in Kleinbuchstaben (a-z).

HTML-Dekodierung

AWS WAF Classic ersetzt HTML-kodierte Zeichen durch unkodierte Zeichen:

- Ersetzt " durch &
- Ersetzt durch ein geschütztes Leerzeichen
- Ersetzt &l t; durch <
- Ersetzt > durch >
- Ersetzt Zeichen im Hexadezimalformat &#xhhhh; mit dem entsprechenden Zeichen
- Ersetzt Zeichen im Dezimalformat &#nnnn; mit dem entsprechenden Zeichen

Leerzeichen normalisieren

AWS WAF Classic ersetzt die folgenden Zeichen durch ein Leerzeichen (Dezimalzahl 32):

- \f, Zeilenvorschubzeichen, Dezimalzahl 12

- \t, Tabulator, Dezimalzahl 9
- \n, Zeilenumbruch, Dezimalzahl 10
- \r, Wagenrücklauf, Dezimalzahl 13
- \v, vertikaler Tabulator, Dezimalzahl 11
- geschütztes Leerzeichen, Dezimalzahl 160

Diese Option ersetzt mehrere aufeinanderfolgende Leerzeichen durch 1 Leerzeichen.

Vereinfachen der Befehlszeile

Verwenden Sie diese Option für Anforderungen mit Befehlszeilen-Befehlen des Betriebssystems, um folgende Transformationen auszuführen:

- Löschen der folgenden Zeichen: \ " ' ^
- Löschen von Leerzeichen vor den folgenden Zeichen: / (
- Ersetzen der folgenden Zeichen durch ein Leerzeichen: , ;
- Ersetzen mehrerer Leerzeichen durch ein Leerzeichen
- Konvertieren von Groß- (A-Z) in Kleinbuchstaben (a-z)

URL-Dekodierung

Dekodieren Sie eine URL-kodierte Anforderung.

Hinzufügen und Löschen von Filtern in einer Cross-Site-Scripting-Übereinstimmungsbedingung

Sie können die Filter in einer Cross-Site-Scripting-Übereinstimmungsbedingung hinzufügen oder löschen. Um einen Filter zu ändern, fügen Sie einen neuen hinzu und löschen den alten.

So fügen Sie Filter in einer Cross-Site-Scripting-Übereinstimmungsbedingung hinzu oder löschen diese

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich Cross-site scripting.
3. Wählen Sie die Bedingung aus, die Sie Filtern hinzufügen oder daraus löschen möchten.

4. Um Filter hinzuzufügen, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie Add filter.
 - b. Geben Sie die entsprechenden Filtereinstellungen an. Weitere Informationen finden Sie unter [Werte, die Sie beim Erstellen oder Bearbeiten von Cross-Site-Scripting-Übereinstimmungsbedingungen angeben](#).
 - c. Wählen Sie Hinzufügen aus.
5. Um Filter zu löschen, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie den Filter aus, den Sie löschen möchten.
 - b. Wählen Sie Delete filter.

Löschen von Cross-Site-Scripting-Übereinstimmungsbedingungen

Wenn Sie eine Cross-Site-Scripting-Übereinstimmungsbedingung löschen möchten, müssen Sie alle Filter in der Bedingung löschen und diese aus allen Regeln löschen, die sie verwenden. Dies wird im Folgenden beschrieben.

So löschen Sie eine Cross-Site Scripting-Übereinstimmungsbedingung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich Cross-site scripting.
3. Wählen Sie im Bereich Cross-site scripting match conditions die Cross-site Scripting-Übereinstimmungsbedingung aus, die Sie löschen möchten.
4. Wählen Sie im rechten Bereich die Registerkarte Associated rules aus.

Wenn die Liste der Regeln, die diese Cross-Site Scripting-Übereinstimmungsbedingung verwenden, leer ist, fahren Sie mit Schritt 6 fort. Wenn die Liste Regeln enthält, notieren Sie sich diese und fahren Sie mit Schritt 5 fort.

5. Um die Cross-Site Scripting-Übereinstimmungsbedingung aus den Regeln, die diese verwenden, zu entfernen, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie im Navigationsbereich Regeln aus.

- b. Wählen Sie den Namen einer Regel aus, die die Cross-Site Scripting-Übereinstimmungsbedingung verwendet, die Sie löschen möchten.
 - c. Wählen Sie im rechten Bereich die Cross-Site Scripting-Übereinstimmungsbedingung aus, die Sie aus der Regel entfernen möchten, und wählen Sie Remove selected condition aus.
 - d. Wiederholen Sie die Schritte b und c für alle übrigen Regeln, die die Cross-Site Scripting-Übereinstimmungsbedingung verwenden, die Sie löschen möchten.
 - e. Wählen Sie im Navigationsbereich Cross-site scripting.
 - f. Wählen Sie im Bereich Cross-site scripting match conditions die Cross-site Scripting-Übereinstimmungsbedingung aus, die Sie löschen möchten.
6. Wählen Sie Löschen aus, um diese Bedingung zu löschen.

Arbeiten mit IP-Übereinstimmungsbedingungen

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Um Webanforderungen basierend auf den IP-Adressen zuzulassen oder zu blockieren, von denen sie stammen, erstellen Sie eine oder mehrere IP-Übereinstimmungsbedingungen. Eine IP-Übereinstimmungsbedingung listet bis zu 10,000 IP-Adressen oder IP-Adressbereiche auf, von denen die Anforderungen stammen. Im weiteren Verlauf des Prozesses können Sie beim Erstellen einer Web-ACL angeben, ob Anforderungen von diesen IP-Adressen zugelassen oder blockiert werden sollen.

Themen

- [Erstellen einer IP-Übereinstimmungsbedingung](#)
- [Bearbeiten von IP-Übereinstimmungsbedingungen](#)
- [Löschen von IP-Übereinstimmungsbedingungen](#)

Erstellen einer IP-Übereinstimmungsbedingung

Wenn Sie möchten, dass einige Webanforderungen zugelassen und andere basierend auf den IP-Adressen, von denen sie stammen, blockiert werden sollen, erstellen Sie jeweils eine IP-Übereinstimmungsbedingung für IP-Adressen, die Sie zulassen und die Sie blockieren möchten.

Note

Wenn Sie einer Regel eine IP-Übereinstimmungsbedingung hinzufügen, können Sie AWS WAF Classic auch so konfigurieren, dass Webanfragen zugelassen oder blockiert werden, die nicht von den IP-Adressen stammen, die Sie in der Bedingung angeben.

So erstellen Sie eine IP-Übereinstimmungsbedingung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich IP addresses aus.
3. Wählen Sie Create condition.
4. Geben Sie einen Namen in das Feld Name ein.

Der Name darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) oder die folgenden Sonderzeichen enthalten: `_! "# ` + * } , . /`. Sie können den Namen einer Bedingung nicht mehr ändern, nachdem Sie sie erstellt haben.

5. Wählen Sie die richtige IP-Version aus und geben Sie eine oder mehrere IP-Adressen mithilfe der CIDR-Notation an. Hier sind einige Beispiele:
 - Für die IPv4-Adresse 192.0.2.44 geben Sie 192.0.2.44/32 ein.
 - Geben Sie für die IPv6-Adresse 0:0:0:0:ffff:c000:22c 0:0:0:0:ffff:c000:22c/128 ein.
 - Für den Bereich von IPv4-Adressen von 192.0.2.0 bis 192.0.2.255 geben Sie 192.0.2.0/24 ein.
 - Um den Bereich der IPv6-Adressen von 2620:0:2d0:200:0:0:0:0 to 2620:0:2d0:200:ffff:ffff:ffff:ffff anzugeben, geben Sie 2620:0:2d0:200::/64 ein.

AWS WAF Classic unterstützt IPv4-Adressbereiche: /8 und jeden Bereich zwischen /16 und /32. AWS WAF Classic unterstützt die IPv6-Adressbereiche: /24, /32, /48, /56, /64 und /128. Weitere Informationen zur CIDR-Notation finden Sie im Wikipedia-Artikel [Classless Inter-Domain Routing](#).

6. Wählen Sie Add another IP address or range.
7. Wenn Sie eine andere IP-Adresse bzw. einen anderen Bereich hinzufügen möchten, wiederholen Sie die Schritte 5 und 6.
8. Wenn Sie alle Werte hinzugefügt haben wählen Sie Create IP match condition.

Bearbeiten von IP-Übereinstimmungsbedingungen

Sie können einen IP-Adressbereich einer IP-Übereinstimmungsbedingung hinzufügen oder ihn löschen. Um einen Bereich zu ändern, fügen Sie eine neue Adresse hinzu und löschen die bisherige Adresse.

So bearbeiten Sie eine IP-Übereinstimmungsbedingung

1. [Melden Sie sich bei der an und öffnen Sie die Konsole unter https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/). [AWS Management Console AWS WAF](#)

Wenn im Navigationsbereich zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich IP addresses aus.
3. Wählen Sie im Bereich IP match conditions die IP-Übereinstimmungsbedingung aus, die Sie bearbeiten möchten.
4. So fügen Sie einen IP-Adressbereich hinzu:
 - a. Wählen Sie im rechten Bereich Add IP address or range.
 - b. Wählen Sie die richtige IP-Version aus und geben Sie einen IP-Adressbereich in der CIDR-Notation ein. Hier sind einige Beispiele:
 - Um die IPv4-Adresse 192.0.2.44 anzugeben, geben Sie 192.0.2.44/32 ein.
 - Um die IPv6-Adresse 0:0:0:0:0:ffff:c000:22c anzugeben, geben Sie 0:0:0:0:0:ffff:c000:22c/128 ein.
 - Um den Bereich der IPv4-Adressen von 192.0.2.0 bis 192.0.2.255 festzulegen, geben Sie 192.0.2.0/24 ein.

- Um den Bereich der IPv6-Adressen von 2620:0:2d0:200:0:0:0:0 to 2620:0:2d0:200:ffff:ffff:ffff:ffff anzugeben, geben Sie 2620:0:2d0:200::/64 ein.

AWS WAF Classic unterstützt IPv4-Adressbereiche: /8 und jeden Bereich zwischen /16 und /32. AWS WAF Classic unterstützt die IPv6-Adressbereiche: /24, /32, /48, /56, /64 und /128. Weitere Informationen zur CIDR-Notation finden Sie im Wikipedia-Artikel [Classless Inter-Domain Routing](#).

- c. Um weitere IP-Adressen hinzuzufügen, wählen Sie Add another IP address (Weitere IP-Adresse hinzufügen) und geben Sie den Wert ein.
 - d. Wählen Sie Hinzufügen aus.
5. So löschen Sie eine IP-Adresse oder einen Bereich:
- a. Wählen Sie im rechten Bereich die Werte aus, die Sie löschen möchten.
 - b. Wählen Sie Delete IP address or range.

Löschen von IP-Übereinstimmungsbedingungen

Wenn Sie eine IP-Übereinstimmungsbedingung löschen möchten, müssen Sie zunächst alle IP-Adressen und Bereiche daraus löschen und die Bedingung aus allen Regeln entfernen, die sie verwenden. Dies wird im Folgenden beschrieben.

So löschen Sie eine IP-Übereinstimmungsbedingung

1. [Melden Sie sich bei der an und öffnen Sie die Konsole unter https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/). [AWS Management Console AWS WAF](#)

Wenn im Navigationsbereich zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich IP addresses aus.
3. Wählen Sie im Bereich IP match conditions die IP-Übereinstimmungsbedingung aus, die Sie löschen möchten.
4. Wählen Sie im rechten Bereich die Registerkarte Rules aus.

Wenn die Liste der Regeln, die diese IP-Übereinstimmungsbedingung verwenden, leer ist, fahren Sie mit Schritt 6 fort. Wenn die Liste Regeln enthält, notieren Sie sich diese und fahren Sie mit Schritt 5 fort.

5. Um die IP-Übereinstimmungsbedingung aus den Regeln, die diese verwenden, zu entfernen, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie im Navigationsbereich Regeln aus.
 - b. Wählen Sie den Namen einer Regel aus, die die IP-Übereinstimmungsbedingung verwendet, die Sie löschen möchten.
 - c. Wählen Sie im rechten Bereich die IP-Übereinstimmungsbedingung aus, die Sie aus der Regel entfernen möchten, und wählen Sie Remove selected condition aus.
 - d. Wiederholen Sie die Schritte b und c für alle übrigen Regeln, die die IP-Übereinstimmungsbedingung verwenden, die Sie löschen möchten.
 - e. Wählen Sie im Navigationsbereich IP match conditions aus.
 - f. Wählen Sie im Bereich IP match conditions die IP-Übereinstimmungsbedingung aus, die Sie löschen möchten.
6. Wählen Sie Löschen aus, um diese Bedingung zu löschen.

Arbeiten mit Geo-Übereinstimmungsbedingungen

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Um Webanforderungen basierend auf den IP-Adressen zuzulassen oder zu blockieren, basierend auf dem Land, von denen sie stammen, erstellen Sie eine oder mehrere Geo-Übereinstimmungsbedingungen. Eine geografische Übereinstimmungsbedingung listet die Länder auf, aus denen Ihre Anfragen stammen. Im weiteren Verlauf des Prozesses können Sie beim Erstellen einer Web-ACL angeben, ob Anforderungen von diesen Ländern zugelassen oder blockiert werden sollen.

Sie können Geo-Match-Bedingungen zusammen mit anderen AWS WAF Classic-Bedingungen oder -Regeln verwenden, um eine ausgeklügelte Filterung zu erstellen. Wenn Sie beispielsweise bestimmte

Länder blockieren möchten, aber dennoch bestimmte IP-Adressen aus diesem Land zulassen möchten, können Sie eine Regel erstellen, die eine Geo-Übereinstimmungsbedingung und eine IP-Übereinstimmungsbedingung enthält. Konfigurieren Sie die Regel so, dass Anforderungen blockiert werden, die aus diesem Land stammen und nicht mit den genehmigten IP-Adressen übereinstimmen. Wenn Sie beispielsweise Ressourcen für Benutzer in einem bestimmten Land priorisieren möchten, können Sie eine Geo-Übereinstimmungsbedingung in zwei verschiedene ratenbasierte Regeln einschließen. Legen Sie für Benutzer im bevorzugten Land eine höhere Ratenbegrenzung fest und legen Sie für alle anderen Benutzer eine niedrigere Ratenbegrenzung fest.

Note

Wenn Sie die CloudFront Geobeschränkungsfunktion verwenden, um ein Land am Zugriff auf Ihre Inhalte zu hindern, wird jede Anfrage aus diesem Land blockiert und nicht an AWS WAF Classic weitergeleitet. Wenn du also Anfragen aufgrund der geografischen Lage und anderer AWS WAF klassischer Bedingungen zulassen oder blockieren möchtest, solltest du die Funktion zur CloudFront geografischen Beschränkung nicht verwenden. Stattdessen sollten Sie eine AWS WAF klassische Geo-Match-Bedingung verwenden.

Themen

- [Erstellen einer Geo-Übereinstimmungsbedingung](#)
- [Bearbeiten von Geo-Übereinstimmungsbedingungen](#)
- [Löschen von Geo-Übereinstimmungsbedingungen](#)

Erstellen einer Geo-Übereinstimmungsbedingung

Wenn Sie möchten, dass einige Webanforderungen zugelassen und andere basierend auf den Geo-Adressen, von denen sie stammen, blockiert werden sollen, erstellen Sie jeweils eine Geo-Übereinstimmungsbedingung für IP-Adressen, die Sie zulassen und die Sie blockieren möchten.

Note

Wenn Sie einer Regel eine Geo-Match-Bedingung hinzufügen, können Sie AWS WAF Classic auch so konfigurieren, dass Webanfragen zugelassen oder blockiert werden, die nicht aus dem Land stammen, das Sie in der Bedingung angegeben haben.

So erstellen Sie eine Geo-Übereinstimmungsbedingung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie die Option aus.

2. Wählen Sie im Navigationsbereich Geo match aus.
3. Wählen Sie Create condition.
4. Geben Sie einen Namen in das Feld Name ein.

Der Name darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) oder die folgenden Sonderzeichen enthalten: `_!@#`+*},./` . Sie können den Namen einer Bedingung nicht mehr ändern, nachdem Sie sie erstellt haben.

5. Region wählen Region.
6. Wählen Sie einen Standorttyp und ein Land. Der Location type (Standorttyp) kann derzeit nur Country (Land) sein.
7. Wählen Sie Add location.
8. Wählen Sie Erstellen.

Bearbeiten von Geo-Übereinstimmungsbedingungen

Sie können Länder zu Ihrer Geo-Übereinstimmungsbedingung hinzufügen oder löschen.

So bearbeiten Sie eine Geo-Übereinstimmungsbedingung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie die Option aus.

2. Wählen Sie im Navigationsbereich Geo match aus.
3. Wählen Sie im Bereich Geo match conditions die Geo-Übereinstimmungsbedingung aus, die Sie bearbeiten möchten.
4. So fügen Sie ein Land hinzu:
 - a. Wählen Sie im rechten Bereich Add filter aus.

- b. Wählen Sie einen Standorttyp und ein Land. Der Location type (Standorttyp) kann derzeit nur Country (Land) sein.
 - c. Wählen Sie Hinzufügen aus.
5. Löschen eines Landes:
- a. Wählen Sie im rechten Bereich die Werte aus, die Sie löschen möchten.
 - b. Wählen Sie Delete filter.

Löschen von Geo-Übereinstimmungsbedingungen

Wenn Sie eine Geo-Übereinstimmungsbedingung löschen möchten, müssen Sie zunächst alle Länder daraus löschen und die Bedingung aus allen Regeln entfernen, die sie verwenden. Dies wird im Folgenden beschrieben.

So löschen Sie eine Geo-Übereinstimmungsbedingung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie die Option aus.

2. Entfernen Sie die Geo-Übereinstimmungsbedingung aus den Regeln, die sie verwenden:
 - a. Wählen Sie im Navigationsbereich Regeln aus.
 - b. Wählen Sie den Namen einer Regel aus, die die Geo-Übereinstimmungsbedingung verwendet, die Sie löschen möchten.
 - c. Wählen Sie im rechten Bereich die Registerkarte Edit rule aus.
 - d. Wählen Sie X neben der Bedingung, die Sie löschen möchten.
 - e. Wählen Sie Aktualisieren.
 - f. Wiederholen Sie das für alle übrigen Regeln, die die Geo-Übereinstimmungsbedingung verwenden, die Sie löschen möchten.
3. Entfernen Sie die Filter aus der Bedingung, die Sie löschen möchten:
 - a. Wählen Sie im Navigationsbereich Geo match aus.
 - b. Klicken Sie auf den Namen der Geo-Übereinstimmungsbedingung, die Sie löschen möchten.

- c. Aktivieren Sie im rechten Fenster das Kontrollkästchen neben Filter, um alle Filter auszuwählen.
 - d. Wählen Sie Delete filter.
4. Wählen Sie im Navigationsbereich Geo match aus.
 5. Wählen Sie im Bereich Geo match conditions die Geo-Übereinstimmungsbedingung aus, die Sie löschen möchten.
 6. Wählen Sie Löschen aus, um diese Bedingung zu löschen.

Arbeiten mit Größenbeschränkungsbedingungen

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Wenn Sie Webanforderungen basierend auf der Länge von bestimmten Teilen zulassen oder blockieren möchten, erstellen Sie eine oder mehrere Größenbeschränkungsbedingungen. Eine Größenbeschränkungsbedingung identifiziert den Teil der Webanfragen, den AWS WAF Classic untersuchen soll, die Anzahl der Byte, nach denen AWS WAF Classic suchen soll, und einen Operator, z. B. größer als (>) oder kleiner als (<). Sie können beispielsweise mithilfe einer Größenbeschränkungsbedingung nach Abfragezeichenfolgen suchen, die länger als 100 Byte sind. Im weiteren Verlauf des Prozesses können Sie beim Erstellen einer Web-ACL angeben, ob Anforderungen basierend auf diesen Einstellungen zugelassen oder blockiert werden sollen.

Beachten Sie, dass AWS WAF Classic nur die ersten 8192 Byte (8 KB) untersucht, wenn Sie AWS WAF Classic so konfigurieren, dass der Hauptteil der Anfrage beispielsweise nach einer bestimmten Zeichenfolge durchsucht wird. Wenn der Text Ihrer Webanforderungen 8192 Byte nicht überschreiten wird, können Sie eine Größenbeschränkungsbedingung erstellen und Anforderungen mit einem Text, der größer als 8.192 Byte ist, blockieren.

Themen

- [Erstellen von Größenbeschränkungsbedingungen](#)
- [Werte, die Sie beim Erstellen oder Bearbeiten von Größenbeschränkungsbedingungen angeben](#)
- [Hinzufügen und Löschen von Filtern in einer Größenbeschränkungsbedingung](#)
- [Löschen von Größenbeschränkungsbedingungen](#)

Erstellen von Größenbeschränkungsbedingungen

Wenn Sie Bedingungen für Größenbeschränkungen erstellen, geben Sie Filter an, die den Teil der Webanfragen identifizieren, für den AWS WAF Classic die Länge auswerten soll. Sie können mehr als einen Filter zu einer Größenbeschränkungsbedingung hinzufügen oder eine separate Bedingung für jeden Filter erstellen. So wirkt sich jede Konfiguration auf das Verhalten von AWS WAF Classic aus:

- Ein Filter pro Größenbeschränkungsbedingung — Wenn Sie einer Regel die separaten Größenbeschränkungsbedingungen hinzufügen und die Regel zu einer Web-ACL hinzufügen, müssen Webanfragen alle Bedingungen erfüllen, damit AWS WAF Classic Anfragen auf der Grundlage der Bedingungen zulässt oder blockiert.

Angenommen Sie erstellen zwei Bedingungen. Eine stimmt mit Webanforderungen überein, deren Abfragezeichenfolgen größer als 100 Byte sind. Die andere stimmt mit Webanforderungen überein, deren Text größer als 1024 Byte ist. Wenn Sie beide Bedingungen zu derselben Regel hinzufügen und die Regel zu einer Web-ACL hinzufügen, erlaubt oder blockiert AWS WAF Classic Anfragen nur, wenn beide Bedingungen erfüllt sind.

- Mehr als ein Filter pro Größenbeschränkungsbedingung — Wenn Sie einer Regel eine Größenbeschränkungsbedingung hinzufügen, die mehrere Filter enthält, und die Regel einer Web-ACL hinzufügen, muss eine Webanforderung nur einem der Filter in der Größenbeschränkungsbedingung entsprechen, damit AWS WAF Classic die Anfrage basierend auf dieser Bedingung zulässt oder blockiert.

Angenommen, Sie erstellen eine Bedingung statt zwei, und die eine Bedingung enthält dieselben zwei Filter wie im vorherigen Beispiel. AWS WAF Classic erlaubt oder blockiert Anfragen, wenn entweder die Abfragezeichenfolge größer als 100 Byte oder der Hauptteil der Anfrage größer als 1024 Byte ist.

Note

Wenn Sie einer Regel eine Größenbeschränkungsbedingung hinzufügen, können Sie AWS WAF Classic auch so konfigurieren, dass Webanfragen zugelassen oder blockiert werden, die nicht den Werten in der Bedingung entsprechen.

So erstellen Sie eine Größenbeschränkungsbedingung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich Size constraints aus.
3. Wählen Sie Create condition.
4. Geben Sie die entsprechenden Filtereinstellungen an. Weitere Informationen finden Sie unter [Werte, die Sie beim Erstellen oder Bearbeiten von Größenbeschränkungsbedingungen angeben](#).
5. Wählen Sie Add another filter.
6. Wenn Sie einen anderen Filter hinzufügen möchten, wiederholen Sie die Schritte 4 und 5.
7. Wenn Sie alle Filter hinzugefügt haben wählen Sie Create size constraint condition.

Werte, die Sie beim Erstellen oder Bearbeiten von Größenbeschränkungsbedingungen angeben

Beim Erstellen oder Aktualisieren einer Größenbeschränkungsbedingung geben Sie die folgenden Werte an:

Name

Geben Sie einen Namen für die Bedingung der Größenbeschränkung ein.

Der Name darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) oder die folgenden Sonderzeichen enthalten: `_! "# +*},./` . Sie können den Namen einer Bedingung nicht mehr ändern, nachdem Sie sie erstellt haben.

Teil der Anforderung, nach dem gefiltert werden soll

Wählen Sie den Teil jeder Webanfrage aus, für den AWS WAF Classic die Länge auswerten soll:

Header

Ein angegebener Anforderungs-Header, wie z. B. der `User-Agent`- oder `Referer`-Header. Wenn Sie Header auswählen, geben Sie den Namen des Headers im Feld Header an.

HTTP-Methode

Die HTTP-Methode, die den Typ des Vorgangs angibt, den die Anfrage vom Ursprung ausführen soll. CloudFront unterstützt die folgenden Methoden: `DELETE`, `GET`, `HEAD`, `OPTIONS`, `PATCH`, `POST`, und `PUT`.

Abfragezeichenfolge

Der Teil einer URL nach einem `?`-Zeichen, sofern vorhanden.

URI

Der URI-Pfad der Anfrage, der die Ressource identifiziert, z. B. `/images/daily-ad.jpg`. Dies beinhaltet nicht die Abfragezeichenfolge oder die Fragmentkomponenten der URI. Informationen dazu finden Sie unter [Uniform Resource Identifier \(URI\): Generic Syntax](#).

Sofern keine Transformation angegeben ist, ist ein URI nicht normalisiert und wird genauso geprüft, wie er im Rahmen der Anfrage vom Client AWS empfangen wird. Eine Transformation formatiert die URI wie vorgegeben neu.

Fließtext

Der Teil einer Anforderung, der zusätzliche Daten enthält, die Sie als HTTP-Anforderungstext an Ihren Webserver senden möchten, wie z. B. Formulardaten.

Einzelner Abfrageparameter (ausschließlich Wert)

Jeder Parameter, den Sie als Teil der Abfragezeichenfolge definiert haben. Wenn die URL beispielsweise `„www.xyz.com? UserName =abc& SalesRegion =seattle“` lautet, können Sie entweder dem Parameter oder einen Filter hinzufügen. `UserNameSalesRegion`

Wenn Sie Einzelner Abfrageparameter (ausschließlich Wert) auswählen, legen Sie auch einen Abfrageparameternamen fest. Dies ist der Parameter in der Abfragezeichenfolge, den Sie überprüfen werden, z. B. `UserName`. Die maximale Länge für den Abfrageparameternamen beträgt 30 Zeichen. Der Abfrageparametername berücksichtigt keine Groß- und Kleinschreibung. Wenn Sie beispielsweise den Namen des Query-Parameters angeben `UserName`, entspricht dies allen Varianten von `UserName`, z. B. `UsERName` und `userName`.

Alle Abfrageparameter (ausschließlich Werte)

Ähnlich wie Einzelner Abfrageparameter (nur Wert), untersucht AWS WAF Classic jedoch nicht den Wert eines einzelnen Parameters, sondern die Werte aller Parameter innerhalb der Abfragezeichenfolge auf die Größenbeschränkung. Wenn die URL beispielsweise „www.xyz.com? Username =abc& SalesRegion =seattle“ lautet und Sie Alle Abfrageparameter (nur Werte) auswählen, löst AWS WAF Classic eine Übereinstimmung mit dem Wert aus, wenn einer der angegebenen Werte die angegebene Größe überschreitet oder diese überschreitet. UsernameSalesRegion

Header (nur wenn "Teil der Filter" auf "Header" festgelegt ist)

Wenn Sie Header für Teil der Anfrage, nach dem gefiltert werden soll, ausgewählt haben, wählen Sie einen Header aus der Liste der allgemeinen Header aus, oder geben Sie den Namen eines Headers ein, für den Classic die Länge auswerten soll. AWS WAF

Vergleichsoperator

Wählen Sie aus, wie AWS WAF Classic die Länge der Abfragezeichenfolge in Webanfragen in Bezug auf den Wert auswerten soll, den Sie für Größe angeben.

Wenn Sie beispielsweise für den Vergleichsoperator Ist größer als auswählen und 100 für Größe eingeben, wertet AWS WAF Classic Webanfragen für eine Abfragezeichenfolge aus, die länger als 100 Byte ist.

Größe

Geben Sie die Länge in Byte ein, auf die AWS WAF Classic in Abfragezeichenfolgen achten soll.

Note

Wenn Sie URI für den Wert von Part of the request to filter on wählen, wird der / in der URI als ein Zeichen gezählt. Der URI-Pfad /logo . jpg ist beispielsweise neun Zeichen lang.

Transformation

Eine Transformation formatiert eine Webanforderung neu, bevor AWS WAF Classic die Länge des angegebenen Teils der Anfrage auswertet. Dadurch werden einige der ungewöhnlichen Formatierungen vermieden, die Angreifer in Webanfragen verwenden, um Classic zu umgehen AWS WAF .

Note

Wenn Sie für Teil der Anfrage, nach der gefiltert werden soll, den Text auswählen, können Sie AWS WAF Classic nicht so konfigurieren, dass eine Transformation durchgeführt wird, da nur die ersten 8192 Byte zur Überprüfung weitergeleitet werden. Sie können Ihren Datenverkehr jedoch weiterhin anhand der Größe des Hauptteils der HTTP-Anfrage filtern und die Transformation Keine angeben. (AWS WAF Classic ermittelt die Länge des Hauptteils aus den Anforderungsheadern.)

Sie können nur einen einzigen Texttransformationstyp angeben.

Transformationen können die folgenden Vorgänge ausführen:

None

AWS WAF Classic führt keine Texttransformationen an der Webanforderung durch, bevor die Länge überprüft wurde.

In Kleinbuchstaben konvertieren

AWS WAF Classic konvertiert Großbuchstaben (A-Z) in Kleinbuchstaben (a-z).

HTML-Dekodierung

AWS WAF Classic ersetzt HTML-kodierte Zeichen durch unkodierte Zeichen:

- Ersetzt `"` durch `&`
- Ersetzt ` ` durch ein geschütztes Leerzeichen
- Ersetzt `<` durch `<`
- Ersetzt `>` durch `>`
- Ersetzt Zeichen im Hexadezimalformat `&#xhhhh;` mit dem entsprechenden Zeichen
- Ersetzt Zeichen im Dezimalformat `&#nnnn;` mit dem entsprechenden Zeichen

Leerzeichen normalisieren

AWS WAF Classic ersetzt die folgenden Zeichen durch ein Leerzeichen (Dezimalzahl 32):

- `\f`, Zeilenvorschubzeichen, Dezimalzahl 12
- `\t`, Tabulator, Dezimalzahl 9
- `\n`, Zeilenumbruch, Dezimalzahl 10
- `\r`, Wagenrücklauf, Dezimalzahl 13

- \v, vertikaler Tabulator, Dezimalzahl 11
- geschütztes Leerzeichen, Dezimalzahl 160

Diese Option ersetzt mehrere aufeinanderfolgende Leerzeichen durch 1 Leerzeichen.

Vereinfachen der Befehlszeile

Verwenden Sie diese Option für Anforderungen mit Befehlszeilen-Befehlen des Betriebssystems, um folgende Transformationen auszuführen:

- Löschen der folgenden Zeichen: \ " ' ^
- Löschen von Leerzeichen vor den folgenden Zeichen: / (
- Ersetzen der folgenden Zeichen durch ein Leerzeichen: , ;
- Ersetzen mehrerer Leerzeichen durch ein Leerzeichen
- Konvertieren von Groß- (A-Z) in Kleinbuchstaben (a-z)

URL-Dekodierung

Dekodieren Sie eine URL-kodierte Anforderung.

Hinzufügen und Löschen von Filtern in einer Größenbeschränkungsbedingung

Sie können einer Größenbeschränkungsbedingung Filter hinzufügen oder daraus löschen. Um einen Filter zu ändern, fügen Sie einen neuen hinzu und löschen den alten.

So fügen Sie einer Größenbeschränkungsbedingung Filter hinzu oder löschen sie

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich Size constraint aus.
3. Wählen Sie die Bedingung aus, die Sie Filtern hinzufügen oder daraus löschen möchten.
4. Um Filter hinzuzufügen, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie Add filter.
 - b. Geben Sie die entsprechenden Filtereinstellungen an. Weitere Informationen finden Sie unter [Werte, die Sie beim Erstellen oder Bearbeiten von Größenbeschränkungsbedingungen angeben](#).

- c. Wählen Sie Hinzufügen aus.
5. Um Filter zu löschen, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie den Filter aus, den Sie löschen möchten.
 - b. Wählen Sie Delete filter.

Löschen von Größenbeschränkungsbedingungen

Wenn Sie eine Größenbeschränkungsbedingung löschen möchten, müssen Sie zuerst alle Filter in der Bedingung löschen und diese aus allen Regeln löschen, die sie verwenden. Dies wird im Folgenden beschrieben.

So löschen Sie eine Größenbeschränkungsbedingung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich Size constraints aus.
3. Wählen Sie im Bereich Size constraint conditions die Größenbeschränkungsbedingung aus, die Sie löschen möchten.
4. Wählen Sie im rechten Bereich die Registerkarte Associated rules aus.

Wenn die Liste der Regeln, die diese Größenbeschränkungsbedingung verwenden, leer ist, fahren Sie mit Schritt 6 fort. Wenn die Liste Regeln enthält, notieren Sie sich diese und fahren Sie mit Schritt 5 fort.

5. Um die Größenbeschränkungsbedingung aus den Regeln, die diese verwenden, zu entfernen, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie im Navigationsbereich Regeln aus.
 - b. Wählen Sie den Namen einer Regel aus, die die Größenbeschränkungsbedingung verwendet, die Sie löschen möchten.
 - c. Wählen Sie im rechten Bereich die Größenbeschränkungsbedingung aus, die Sie aus der Regel entfernen möchten, und wählen Sie Remove selected condition aus.
 - d. Wiederholen Sie die Schritte b und c für alle übrigen Regeln, die die Größenbeschränkungsbedingung verwenden, die Sie löschen möchten.

- e. Wählen Sie im Navigationsbereich Size constraint aus.
 - f. Wählen Sie im Bereich Size constraint conditions die Größenbeschränkungsbedingung aus, die Sie löschen möchten.
6. Wählen Sie Löschen aus, um diese Bedingung zu löschen.

Arbeiten mit SQL Injections-Übereinstimmungsbedingungen

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Angreifer versuchen manchmal, schädlichen SQL-Code in Webanforderungen einzufügen, um Daten aus Ihrer Datenbank zu extrahieren. Um Webanforderungen basierend darauf, ob sie möglicherweise schädlichen SQL-Code enthalten, zuzulassen oder zu blockieren, erstellen Sie eine oder mehrere SQL Injections-Übereinstimmungsbedingungen. Eine SQL-Injection-Match-Bedingung identifiziert den Teil der Webanforderungen, wie z. B. den URI-Pfad oder die Abfragezeichenfolge, den AWS WAF Classic untersuchen soll. Im weiteren Verlauf des Prozesses können Sie beim Erstellen einer Web-ACL angeben, ob Sie Anforderungen zulassen oder blockieren möchten, die schädlichen SQL-Code enthalten.

Themen

- [Erstellen einer SQL Injections-Übereinstimmungsbedingung](#)
- [Werte, die Sie beim Erstellen oder Bearbeiten von SQL Injections-Übereinstimmungsbedingungen angeben](#)
- [Hinzufügen und Löschen von Filtern in einer SQL Injections-Übereinstimmungsbedingung](#)
- [Löschen von SQL Injections-Übereinstimmungsbedingungen](#)

Erstellen einer SQL Injections-Übereinstimmungsbedingung

Wenn Sie Vergleichsbedingungen für SQL-Injection erstellen, geben Sie Filter an, die den Teil der Webanfragen angeben, den AWS WAF Classic auf bösartigen SQL-Code untersuchen soll, z. B. den URI oder die Abfragezeichenfolge. Sie können mehrere Filter zu einer SQL Injections-Übereinstimmungsbedingung hinzufügen oder eine separate Bedingung für jeden Filter erstellen. So wirkt sich jede Konfiguration auf das Verhalten von AWS WAF Classic aus:

- Mehr als ein Filter pro SQL-Injection-Übereinstimmungsbedingung (empfohlen) — Wenn Sie einer Regel eine SQL-Injection-Übereinstimmungsbedingung hinzufügen, die mehrere Filter enthält, und die Regel einer Web-ACL hinzufügen, muss eine Webanforderung nur einem der Filter in der SQL-Injection-Abgleichsbedingung entsprechen, damit AWS WAF Classic die Anfrage basierend auf dieser Bedingung zulässt oder blockiert.

Beispiel: Sie erstellen eine SQL Injections-Übereinstimmungsbedingung, die zwei Filter enthält. Ein Filter weist AWS WAF Classic an, den URI auf bösartigen SQL-Code zu überprüfen, und der andere weist AWS WAF Classic an, die Abfragezeichenfolge zu überprüfen. AWS WAF Classic lässt Anfragen zu oder blockiert sie, wenn sie bösartigen SQL-Code entweder im URI oder in der Abfragezeichenfolge zu enthalten scheinen.

- Ein Filter pro SQL-Injection-Übereinstimmungsbedingung — Wenn Sie die separaten SQL-Injection-Abgleichsbedingungen zu einer Regel hinzufügen und die Regel zu einer Web-ACL hinzufügen, müssen Webanfragen alle Bedingungen erfüllen, damit AWS WAF Classic Anfragen auf der Grundlage der Bedingungen zulassen oder blockieren kann.

Angenommen Sie erstellen zwei Bedingungen, die jeweils einen der beiden Filter im vorherigen Beispiel enthalten. Wenn Sie beide Bedingungen zu derselben Regel hinzufügen und die Regel zu einer Web-ACL hinzufügen, erlaubt oder blockiert AWS WAF Classic Anfragen nur, wenn sowohl der URI als auch die Abfragezeichenfolge bösartigen SQL-Code zu enthalten scheinen.

Note

Wenn Sie einer Regel eine SQL-Injection-Übereinstimmungsbedingung hinzufügen, können Sie AWS WAF Classic auch so konfigurieren, dass Webanfragen zugelassen oder blockiert werden, die keinen bösartigen SQL-Code zu enthalten scheinen.

So erstellen Sie eine SQL Injections-Übereinstimmungsbedingung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich SQL injection aus.
3. Wählen Sie Create condition.
4. Geben Sie die entsprechenden Filtereinstellungen an. Weitere Informationen finden Sie unter [Werte, die Sie beim Erstellen oder Bearbeiten von SQL Injections-Übereinstimmungsbedingungen angeben](#).
5. Wählen Sie Add another filter.
6. Wenn Sie einen anderen Filter hinzufügen möchten, wiederholen Sie die Schritte 4 und 5.
7. Wählen Sie nach dem Hinzufügen der Filter Erstellen aus.

Werte, die Sie beim Erstellen oder Bearbeiten von SQL Injections-Übereinstimmungsbedingungen angeben

Beim Erstellen oder Aktualisieren einer SQL Injections-Übereinstimmungsbedingung geben Sie die folgenden Werte an:

Name

Der Name der SQL Injections-Übereinstimmungsbedingung.

Der Name darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) oder die folgenden Sonderzeichen enthalten: `_!@#`+*},./` . Sie können den Namen einer Bedingung nicht mehr ändern, nachdem Sie sie erstellt haben.

Teil der Anforderung, nach dem gefiltert werden soll

Wählen Sie den Teil jeder Webanfrage aus, den AWS WAF Classic auf böartigen SQL-Code untersuchen soll:

Header

Ein angegebener Anforderungs-Header, wie z. B. der `User-Agent`- oder `Referer`-Header. Wenn Sie Header auswählen, geben Sie den Namen des Headers im Feld Header an.

HTTP-Methode

Die HTTP-Methode, die die Art des Vorgangs angibt, zu dessen Ausführung die Anfrage den Ursprung auffordert. CloudFront unterstützt die folgenden Methoden: DELETE, GET, HEAD, OPTIONS, PATCH, POST, und PUT.

Abfragezeichenfolge

Der Teil einer URL nach einem ?-Zeichen, sofern vorhanden.

Note

Für SQL Injections-Übereinstimmungsbedingungen empfehlen wir, dass Sie All query parameters (values only) (Alle Abfrageparameter (nur Werte) anstelle von Query string (Abfragezeichenfolge) für Part of the request to filter on (Teil der Anforderung, nach dem gefiltert werden soll) auswählen.

URI

Der URI-Pfad der Anfrage, der die Ressource identifiziert, /images/daily-ad.jpg z. B. Dies beinhaltet nicht die Abfragezeichenfolge oder die Fragmentkomponenten der URI. Informationen dazu finden Sie unter [Uniform Resource Identifier \(URI\): Generic Syntax](#).

Sofern keine Transformation angegeben ist, ist ein URI nicht normalisiert und wird genauso geprüft, wie er im Rahmen der Anfrage vom Client AWS empfangen wird. Eine Transformation formatiert die URI wie vorgegeben neu.

Fließtext

Der Teil einer Anforderung, der zusätzliche Daten enthält, die Sie als HTTP-Anforderungstext an Ihren Webserver senden möchten, wie z. B. Formulardaten.

Note

Wenn Sie für den Wert Teil der Anforderung, nach dem gefiltert werden soll, Body wählen, untersucht AWS WAF Classic nur die ersten 8192 Byte (8 KB). Um Anfragen zuzulassen oder zu blockieren, deren Hauptteil länger als 8192 Byte ist, können Sie eine Größenbeschränkungsbedingung erstellen. (AWS WAF Classic ermittelt die Länge des Hauptteils aus den Anforderungsheadern.) Weitere Informationen finden Sie unter [Arbeiten mit Größenbeschränkungsbedingungen](#).

Einzelner Abfrageparameter (ausschließlich Wert)

Jeder Parameter, den Sie als Teil der Abfragezeichenfolge definiert haben. Wenn die URL beispielsweise „www.xyz.com? UserName =abc& SalesRegion =seattle“ lautet, können Sie entweder dem Parameter oder einen Filter hinzufügen. UserNameSalesRegion

Wenn Sie Einzelner Abfrageparameter (ausschließlich Wert) auswählen, legen Sie auch einen Abfrageparameternamen fest. Dies ist der Parameter in der Abfragezeichenfolge, den Sie überprüfen werden, z. B. oder. UserNameSalesRegion Die maximale Länge für den Abfrageparameternamen beträgt 30 Zeichen. Der Abfrageparametername berücksichtigt keine Groß- und Kleinschreibung. Wenn Sie beispielsweise den Namen des Query-Parameters angeben UserName, entspricht dies allen Varianten von UserName, z. B. UsERName und userName.

Alle Abfrageparameter (ausschließlich Werte)

Ähnlich wie Einzelner Abfrageparameter (nur Wert), untersucht AWS WAF Classic jedoch nicht den Wert eines einzelnen Parameters, sondern den Wert aller Parameter innerhalb der Abfragezeichenfolge auf möglichen bösartigen SQL-Code. Wenn die URL beispielsweise „www.xyz.com? UserName =abc& SalesRegion =seattle“ lautet und Sie Alle Abfrageparameter (nur Werte) wählen, löst AWS WAF Classic eine Übereinstimmung aus, wenn der Wert von einem oder mehreren möglichen bösartigen SQL-Code enthält. UserNameSalesRegion

Header

Wenn Sie Header für Teil der Anfrage, nach der gefiltert werden soll, ausgewählt haben, wählen Sie einen Header aus der Liste der allgemeinen Header aus, oder geben Sie den Namen eines Headers ein, den Classic auf bösartigen SQL-Code untersuchen soll AWS WAF .

Transformation

Eine Transformation formatiert eine Webanforderung neu, bevor AWS WAF Classic die Anfrage überprüft. Dadurch werden einige der ungewöhnlichen Formatierungen vermieden, die Angreifer in Webanfragen verwenden, um Classic zu umgehen AWS WAF .

Sie können nur einen einzigen Texttransformationstyp angeben.

Transformationen können die folgenden Vorgänge ausführen:

None

AWS WAF Classic führt keine Texttransformationen an der Webanforderung durch, bevor überprüft wird, ob die Zeichenfolge in Value übereinstimmt.

In Kleinbuchstaben konvertieren

AWS WAF Classic konvertiert Großbuchstaben (A-Z) in Kleinbuchstaben (a-z).

HTML-Dekodierung

AWS WAF Classic ersetzt HTML-kodierte Zeichen durch unkodierte Zeichen:

- Ersetzt `"` durch `&`
- Ersetzt ` ` durch ein geschütztes Leerzeichen
- Ersetzt `<` durch `<`
- Ersetzt `>` durch `>`
- Ersetzt Zeichen im Hexadezimalformat `&#xhhhh;` mit dem entsprechenden Zeichen
- Ersetzt Zeichen im Dezimalformat `&#nnnn;` mit dem entsprechenden Zeichen

Leerzeichen normalisieren

AWS WAF Classic ersetzt die folgenden Zeichen durch ein Leerzeichen (Dezimalzahl 32):

- `\f`, Zeilenvorschubzeichen, Dezimalzahl 12
- `\t`, Tabulator, Dezimalzahl 9
- `\n`, Zeilenumbruch, Dezimalzahl 10
- `\r`, Wagenrücklauf, Dezimalzahl 13
- `\v`, vertikaler Tabulator, Dezimalzahl 11
- geschütztes Leerzeichen, Dezimalzahl 160

Diese Option ersetzt mehrere aufeinanderfolgende Leerzeichen durch 1 Leerzeichen.

Vereinfachen der Befehlszeile

Verwenden Sie diese Option für Anforderungen mit Befehlszeilen-Befehlen des Betriebssystems, um folgende Transformationen auszuführen:

- Löschen der folgenden Zeichen: `\ " ' ^`
- Löschen von Leerzeichen vor den folgenden Zeichen: `/ (`
- Ersetzen der folgenden Zeichen durch ein Leerzeichen: `, ;`
- Ersetzen mehrerer Leerzeichen durch ein Leerzeichen
- Konvertieren von Groß- (A-Z) in Kleinbuchstaben (a-z)

URL-Dekodierung

Dekodieren Sie eine URL-kodierte Anforderung.

Hinzufügen und Löschen von Filtern in einer SQL Injections-Übereinstimmungsbedingung

Sie können einer SQL Injections-Übereinstimmungsbedingung Filter hinzufügen oder daraus löschen. Um einen Filter zu ändern, fügen Sie einen neuen hinzu und löschen den alten.

So fügen Sie einer SQL Injections-Bedingung Filter hinzu oder löschen sie

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich SQL injection aus.
3. Wählen Sie die Bedingung aus, die Sie Filtern hinzufügen oder daraus löschen möchten.
4. Um Filter hinzuzufügen, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie Add filter.
 - b. Geben Sie die entsprechenden Filtereinstellungen an. Weitere Informationen finden Sie unter [Werte, die Sie beim Erstellen oder Bearbeiten von SQL Injections-Übereinstimmungsbedingungen angeben](#).
 - c. Wählen Sie Hinzufügen aus.
5. Um Filter zu löschen, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie den Filter aus, den Sie löschen möchten.
 - b. Wählen Sie Delete filter.

Löschen von SQL Injections-Übereinstimmungsbedingungen

Wenn Sie eine SQL Injections-Übereinstimmungsbedingung löschen möchten, müssen Sie zuerst alle Filter in der Bedingung löschen und diese aus allen Regeln löschen, die sie verwenden. Dies wird im Folgenden beschrieben.

So löschen Sie eine SQL Injections-Übereinstimmungsbedingung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich SQL injection aus.
3. Wählen Sie im Bereich SQL injection match conditions die SQL Injections-Übereinstimmungsbedingung aus, die Sie löschen möchten.
4. Wählen Sie im rechten Bereich die Registerkarte Associated rules aus.

Wenn die Liste der Regeln, die diese SQL Injections-Übereinstimmungsbedingung verwenden, leer ist, fahren Sie mit Schritt 6 fort. Wenn die Liste Regeln enthält, notieren Sie sich diese und fahren Sie mit Schritt 5 fort.

5. Um die SQL Injections-Übereinstimmungsbedingung aus den Regeln, die diese verwenden, zu entfernen, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie im Navigationsbereich Regeln aus.
 - b. Wählen Sie den Namen einer Regel aus, die die SQL Injections-Übereinstimmungsbedingung verwendet, die Sie löschen möchten.
 - c. Wählen Sie im rechten Bereich die SQL Injections-Übereinstimmungsbedingung aus, die Sie aus der Regel entfernen möchten, und wählen Sie Remove selected condition aus.
 - d. Wiederholen Sie die Schritte b und c für alle übrigen Regeln, die die SQL Injections-Übereinstimmungsbedingung verwenden, die Sie löschen möchten.
 - e. Wählen Sie im Navigationsbereich SQL injection aus.
 - f. Wählen Sie im Bereich SQL injection match conditions die SQL Injections-Übereinstimmungsbedingung aus, die Sie löschen möchten.
6. Wählen Sie Löschen aus, um diese Bedingung zu löschen.

Arbeiten mit Zeichenfolgen-Übereinstimmungsbedingungen

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November

2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Wenn Sie Webanforderungen basierend auf darin enthaltenen Zeichenfolgen zulassen oder blockieren möchten, erstellen Sie eine oder mehrere Zeichenfolgen-Übereinstimmungsbedingungen. Eine Bedingung für die Übereinstimmung mit einer Zeichenfolge identifiziert die Zeichenfolge, nach der Sie suchen möchten, und den Teil der Webanforderungen, wie z. B. einen angegebenen Header oder die Abfragezeichenfolge, den AWS WAF Classic nach der Zeichenfolge durchsuchen soll. Im weiteren Verlauf des Prozesses können Sie beim Erstellen einer Web-ACL angeben, ob Anforderungen, die die Zeichenfolge enthalten, zugelassen oder blockiert werden sollen.

Themen

- [Erstellen einer Zeichenfolgen-Übereinstimmungsbedingung](#)
- [Werte, die Sie beim Erstellen oder Bearbeiten von Zeichenfolgen-Übereinstimmungsbedingungen angeben](#)
- [Hinzufügen und Löschen von Filtern in einer Zeichenfolgen-Übereinstimmungsbedingung](#)
- [Löschen von Zeichenfolgen-Übereinstimmungsbedingungen](#)

Erstellen einer Zeichenfolgen-Übereinstimmungsbedingung

Wenn Sie Bedingungen für den Abgleich von Zeichenfolgen erstellen, geben Sie Filter an, die die Zeichenfolge, nach der Sie suchen möchten, und den Teil der Webanfragen identifizieren, den AWS WAF Classic nach dieser Zeichenfolge durchsuchen soll, z. B. den URI oder die Abfragezeichenfolge. Sie können einer Zeichenfolgen-Übereinstimmungsbedingung mehrere Filter hinzufügen oder eine separate Bedingung für jeden Filter erstellen. So wirkt sich jede Konfiguration auf das Verhalten von AWS WAF Classic aus:

- Ein Filter pro Übereinstimmungsbedingung für Zeichenfolgen — Wenn Sie einer Regel die separaten Bedingungen für den Abgleich von Zeichenfolgen hinzufügen und die Regel einer Web-ACL hinzufügen, müssen Webanfragen alle Bedingungen erfüllen, damit AWS WAF Classic Anfragen auf der Grundlage der Bedingungen zulässt oder blockiert.

Angenommen Sie erstellen zwei Bedingungen. Eine Bedingung stimmt mit Webanforderungen überein, die den Wert BadBot im User-Agent-Header enthalten. Die andere stimmt mit

Webanforderungen überein, die den Wert `BadParameter` in Abfragezeichenfolgen enthalten. Wenn Sie beide Bedingungen zu derselben Regel hinzufügen und die Regel zu einer Web-ACL hinzufügen, erlaubt oder blockiert AWS WAF Classic Anfragen nur, wenn sie beide Werte enthalten.

- Mehr als ein Filter pro Übereinstimmungsbedingung für eine Zeichenfolge — Wenn Sie einer Regel eine Bedingung für die Übereinstimmung mit Zeichenfolgen hinzufügen, die mehrere Filter enthält, und die Regel einer Web-ACL hinzufügen, muss eine Webanforderung nur einem der Filter in der Bedingung für die Übereinstimmung mit Zeichenfolgen entsprechen, damit AWS WAF Classic die Anfrage auf der Grundlage einer Bedingung zulässt oder blockiert.

Angenommen, Sie erstellen eine Bedingung statt zwei, und die eine Bedingung enthält dieselben zwei Filter wie im vorherigen Beispiel. AWS WAF Classic erlaubt oder blockiert Anfragen, wenn sie entweder `BadBot` im `User-Agent` Header oder `BadParameter` in der Abfragezeichenfolge enthalten sind.

Note

Wenn Sie einer Regel eine Bedingung für die Übereinstimmung mit Zeichenfolgen hinzufügen, können Sie AWS WAF Classic auch so konfigurieren, dass Webanfragen zugelassen oder blockiert werden, die nicht den Werten in der Bedingung entsprechen.

So erstellen Sie eine Zeichenfolgen-Übereinstimmungsbedingung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich String and regex matching aus.
3. Wählen Sie Create condition.
4. Geben Sie die entsprechenden Filtereinstellungen an. Weitere Informationen finden Sie unter [Werte, die Sie beim Erstellen oder Bearbeiten von Zeichenfolgen-Übereinstimmungsbedingungen angeben](#).
5. Wählen Sie Add filter.
6. Wenn Sie einen anderen Filter hinzufügen möchten, wiederholen Sie die Schritte 4 und 5.

7. Wählen Sie nach dem Hinzufügen der Filter Erstellen aus.

Werte, die Sie beim Erstellen oder Bearbeiten von Zeichenfolgen-Übereinstimmungsbedingungen angeben

Beim Erstellen oder Aktualisieren einer Zeichenfolgen-Übereinstimmungsbedingung geben Sie die folgenden Werte an:

Name

Geben Sie einen Namen für die Zeichenfolgen-Abgleichsbedingung ein. Der Name darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) oder die folgenden Sonderzeichen enthalten: `_! "# ` + * } , / .`. Sie können den Namen einer Bedingung nicht mehr ändern, nachdem Sie sie erstellt haben.

Typ

Wählen Sie String match.

Teil der Anforderung, nach dem gefiltert werden soll

Wählen Sie den Teil jeder Webanfrage aus, den AWS WAF Classic auf die Zeichenfolge überprüfen soll, die Sie im Feld Passender Wert angegeben haben:

Header

Ein angegebener Anforderungs-Header, wie z. B. der `User-Agent`- oder `Referer`-Header. Wenn Sie Header auswählen, geben Sie den Namen des Headers im Feld Header an.

HTTP-Methode

Die HTTP-Methode, die den Typ des Vorgangs angibt, den die Anfrage vom Ursprung ausführen soll. CloudFront unterstützt die folgenden Methoden: `DELETE`, `GET`, `HEAD`, `OPTIONS`, `PATCH`, `POST`, und `PUT`.

Abfragezeichenfolge

Der Teil einer URL nach einem `?`-Zeichen, sofern vorhanden.

URI

Der URI-Pfad der Anfrage, der die Ressource identifiziert, `/images/daily-ad.jpg` z. B. Dies beinhaltet nicht die Abfragezeichenfolge oder die Fragmentkomponenten der URI. Informationen dazu finden Sie unter [Uniform Resource Identifier \(URI\): Generic Syntax](#).

Sofern keine Transformation angegeben ist, ist ein URI nicht normalisiert und wird genauso geprüft, wie er im Rahmen der Anfrage vom Client AWS empfangen wird. Eine Transformation formatiert die URI wie vorgegeben neu.

Fließtext

Der Teil einer Anforderung, der zusätzliche Daten enthält, die Sie als HTTP-Anforderungstext an Ihren Webserver senden möchten, wie z. B. Formulardaten.

Note

Wenn Sie für den Wert Teil der Anforderung, nach dem gefiltert werden soll, Body wählen, untersucht AWS WAF Classic nur die ersten 8192 Byte (8 KB). Um Anfragen zuzulassen oder zu blockieren, deren Hauptteil länger als 8192 Byte ist, können Sie eine Größenbeschränkungsbedingung erstellen. (AWS WAF Classic ermittelt die Länge des Hauptteils aus den Anforderungsheadern.) Weitere Informationen finden Sie unter [Arbeiten mit Größenbeschränkungsbedingungen](#).

Einzelner Abfrageparameter (ausschließlich Wert)

Jeder Parameter, den Sie als Teil der Abfragezeichenfolge definiert haben. Wenn die URL beispielsweise „www.xyz.com? UserName =abc& SalesRegion =seattle“ lautet, können Sie entweder dem Parameter oder einen Filter hinzufügen. UserNameSalesRegion

Wenn doppelte Parameter in der Abfragezeichenfolge enthalten sind, werden die Werte als "ODER" gewertet. Das heißt, dass auch nur einer der Werte ausreicht, um eine Übereinstimmung auszulösen. Beispiel: In der URL „www.xyz.com? SalesRegion =boston& SalesRegion =seattle“ löst entweder „boston“ oder „seattle“ im Feld Passender Wert eine Übereinstimmung aus.

Wenn Sie Einzelner Abfrageparameter (ausschließlich Wert) auswählen, legen Sie auch einen Abfrageparameternamen fest. Dies ist der Parameter in der Abfragezeichenfolge, den Sie überprüfen werden, z. B. oder. UserNameSalesRegion Die maximale Länge für den Abfrageparameternamen beträgt 30 Zeichen. Der Abfrageparametername berücksichtigt keine Groß- und Kleinschreibung. Wenn Sie beispielsweise den Namen des Query-Parameters angeben UserName, entspricht dies allen Varianten von UserName, z. B. UsERName und userName.

Alle Abfrageparameter (ausschließlich Werte)

Ähnlich wie Einzelner Abfrageparameter (nur Wert), überprüft AWS WAF Classic jedoch nicht den Wert eines einzelnen Parameters, sondern überprüft den Wert aller Parameter innerhalb der Abfragezeichenfolge auf den passenden Wert. Wenn die URL beispielsweise „www.xyz.com? Username =abc& SalesRegion =seattle“ lautet und Sie Alle Abfrageparameter (nur Werte) auswählen, löst AWS WAF Classic eine Übereinstimmung aus, wenn der Wert von einem oder Username als abzugleichender Wert angegeben ist. SalesRegion

Header (nur wenn "Teil der Filter" auf "Header" festgelegt ist)

Wenn Sie in der Liste „Teil der Anforderung, nach der gefiltert werden soll“ die Option „Kopfzeile“ ausgewählt haben, wählen Sie eine Kopfzeile aus der Liste der allgemeinen Kopfzeilen aus, oder geben Sie den Namen einer Kopfzeile ein, die Classic untersuchen soll. AWS WAF

Übereinstimmungstyp

Wählen Sie in dem Teil der Anfrage, den AWS WAF Classic untersuchen soll, aus, wo die Zeichenfolge im Feld Abgleichender Wert erscheinen muss, damit sie diesem Filter entspricht:

Enthält

Die Zeichenfolge befindet sich an einer beliebigen Position innerhalb des angegebenen Anforderungsteils.

Enthält Wort

Der angegebene Teil der Webanforderungen muss Value to match enthalten und Value to match darf nur alphanumerische Zeichen oder Unterstriche (A-Z, a-z, 0-9 oder _) enthalten. Außerdem muss Value to match ein Wort sein und eines der folgenden Kriterien erfüllen:

- Value to match entspricht genau dem Wert des angegebenen Teils der Webanforderung, wie zum Beispiel dem Wert eines Headers.
- Value to match befindet sich am Anfang des angegebenen Teils der Webanforderung, gefolgt von einem Zeichen, das kein alphanumerisches Zeichen und kein Unterstrich () ist, z. B. BadBot ; .
- Value to match befindet sich am Ende des angegebenen Teils der Webanforderung, nach von einem Zeichen, das kein alphanumerisches Zeichen und kein Unterstrich () ist, z. B. ;BadBot.
- Value to match befindet sich in der Mitte des angegebenen Teils der Webanforderung und es geht ein Zeichen voraus bzw. folgt ein Zeichen, das kein alphanumerisches Zeichen und kein Unterstrich () ist, z. B. -BadBot ; .

Stimmt genau überein

Die Zeichenfolge und der Wert des angegebenen Teils der Anforderung sind identisch.

Beginnt mit

Die Zeichenfolge befindet sich am Anfang des angegebenen Teils der Anforderung.

Endet mit

Die Zeichenfolge befindet sich am Ende des angegebenen Teils der Anforderung.

Transformation

Eine Transformation formatiert eine Webanforderung neu, bevor AWS WAF Classic die Anfrage überprüft. Dadurch werden einige der ungewöhnlichen Formatierungen vermieden, die Angreifer in Webanfragen verwenden, um Classic zu umgehen AWS WAF .

Sie können nur einen einzigen Texttransformationstyp angeben.

Transformationen können die folgenden Vorgänge ausführen:

None

AWS WAF Classic führt keine Texttransformationen an der Webanforderung durch, bevor überprüft wird, ob die Zeichenfolge in Value übereinstimmt.

In Kleinbuchstaben konvertieren

AWS WAF Classic konvertiert Großbuchstaben (A-Z) in Kleinbuchstaben (a-z).

HTML-Dekodierung

AWS WAF Classic ersetzt HTML-kodierte Zeichen durch unkodierte Zeichen:

- Ersetzt " durch &
- Ersetzt durch ein geschütztes Leerzeichen
- Ersetzt < durch <
- Ersetzt > durch >
- Ersetzt Zeichen im Hexadezimalformat &#xhhhh; mit dem entsprechenden Zeichen
- Ersetzt Zeichen im Dezimalformat &#nnnn; mit dem entsprechenden Zeichen

Leerzeichen normalisieren

AWS WAF Classic ersetzt die folgenden Zeichen durch ein Leerzeichen (Dezimalzahl 32):

- \f, Zeilenvorschubzeichen, Dezimalzahl 12
- \t, Tabulator, Dezimalzahl 9
- \n, Zeilenumbruch, Dezimalzahl 10
- \r, Wagenrücklauf, Dezimalzahl 13
- \v, vertikaler Tabulator, Dezimalzahl 11
- geschütztes Leerzeichen, Dezimalzahl 160

Diese Option ersetzt mehrere aufeinanderfolgende Leerzeichen durch 1 Leerzeichen.

Vereinfachen der Befehlszeile

Wenn Sie befürchten, dass Angreifer einen Befehlszeilen-Befehl des Betriebssystems einfügen und diesen Befehl ganz oder teilweise durch ungewöhnliche Formatierungen verbergen, verwenden Sie diese Option, um folgende Transformationen auszuführen:

- Löschen der folgenden Zeichen: \ " ' ^
- Löschen von Leerzeichen vor den folgenden Zeichen: / (
- Ersetzen der folgenden Zeichen durch ein Leerzeichen: , ;
- Ersetzen mehrerer Leerzeichen durch ein Leerzeichen
- Konvertieren von Groß- (A-Z) in Kleinbuchstaben (a-z)

URL-Dekodierung

Dekodieren Sie eine URL-kodierte Anforderung.

Der Wert ist base64-kodiert

Aktivieren Sie dieses Kontrollkästchen, wenn der Wert in Value to match base64-kodiert ist. Verwenden Sie die base64-Kodierung, um nicht druckbare Zeichen wie z. B. Tabulatoren und Zeilenumbrüche anzugeben, die Angreifer in ihre Anforderungen aufnehmen.

Wert, der zugeordnet werden soll

Geben Sie den Wert an, nach dem AWS WAF Classic in Webanfragen suchen soll. Die maximale Länge beträgt 50 Byte. Wenn Sie den Wert mit der base64-Kodierung verschlüsseln, gilt das 50-Byte-Limit für den Wert vor der Kodierung.

Hinzufügen und Löschen von Filtern in einer Zeichenfolgen-Übereinstimmungsbedingung

Sie können einer Zeichenfolgen-Übereinstimmungsbedingung Filter hinzufügen oder daraus löschen. Um einen Filter zu ändern, fügen Sie einen neuen hinzu und löschen den alten.

So fügen Sie einer Zeichenfolgen-Übereinstimmungsbedingung Filter hinzu bzw. löschen sie

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich String and regex matching aus.
3. Wählen Sie die Bedingung aus, die Sie Filtern hinzufügen oder daraus löschen möchten.
4. Um Filter hinzuzufügen, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie Add filter.
 - b. Geben Sie die entsprechenden Filtereinstellungen an. Weitere Informationen finden Sie unter [Werte, die Sie beim Erstellen oder Bearbeiten von Zeichenfolgen-Übereinstimmungsbedingungen angeben](#).
 - c. Wählen Sie Hinzufügen aus.
5. Um Filter zu löschen, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie den Filter aus, den Sie löschen möchten.
 - b. Wählen Sie Delete Filter.

Löschen von Zeichenfolgen-Übereinstimmungsbedingungen

Wenn Sie eine Zeichenfolgen-Übereinstimmungsbedingung löschen möchten, müssen Sie zuerst alle Filter in der Bedingung löschen und diese aus allen Regeln löschen, die sie verwenden. Dies wird im Folgenden beschrieben.

So löschen Sie eine Zeichenfolgen-Übereinstimmungsbedingung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Entfernen Sie die Zeichenfolgen-Übereinstimmungsbedingung aus den Regeln, die sie verwenden:
 - a. Wählen Sie im Navigationsbereich Regeln aus.

- b. Wählen Sie den Namen einer Regel aus, die die Zeichenfolgen-Übereinstimmungsbedingung verwendet, die Sie löschen möchten.
 - c. Wählen Sie im rechten Bereich die Registerkarte Edit rule aus.
 - d. Wählen Sie X neben der Bedingung, die Sie löschen möchten.
 - e. Wählen Sie Aktualisieren.
 - f. Wiederholen Sie die Schritte b und c für alle übrigen Regeln, die die Zeichenfolgen-Übereinstimmungsbedingung verwenden, die Sie löschen möchten.
3. Entfernen Sie die Filter aus der Bedingung, die Sie löschen möchten:
 - a. Wählen Sie im Navigationsbereich String and regex matching aus.
 - b. Klicken Sie auf den Namen der Zeichenfolgen-Übereinstimmungsbedingung, die Sie löschen möchten.
 - c. Aktivieren Sie im rechten Fenster das Kontrollkästchen neben Filter, um alle Filter auszuwählen.
 - d. Wählen Sie Delete filter.
 4. Wählen Sie im Navigationsbereich String and regex matching aus.
 5. Wählen Sie im Bereich String and regex match conditions die Zeichenfolgen-Übereinstimmungsbedingung aus, die Sie löschen möchten.
 6. Wählen Sie Löschen aus, um diese Bedingung zu löschen.

Arbeiten mit Regex-Übereinstimmungsbedingungen

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Wenn Sie Webanfragen basierend auf Zeichenfolgen zulassen oder blockieren möchten, die mit einem Muster eines regulären Ausdrucks (regex) übereinstimmen, das in den Anfragen erscheint, erstellen Sie eine oder mehrere regex-Abgleichsbedingungen. Eine Regex-

Übereinstimmungsbedingung ist eine Art von Übereinstimmungsbedingung für Zeichenketten, die das Muster identifiziert, nach dem Sie suchen möchten, und den Teil von Webanfragen, wie z. B. einen angegebenen Header oder die Abfragezeichenfolge, den AWS WAF Classic auf das Muster untersuchen soll. Im weiteren Verlauf des Prozesses können Sie beim Erstellen einer Web-ACL angeben, ob Anforderungen, die das Muster enthalten, zugelassen oder blockiert werden sollen.

Themen

- [Erstellen einer Regex-Übereinstimmungsbedingung](#)
- [Werte, die Sie angeben, wenn Sie Abgleichsbedingungen erstellen oder bearbeiten RegEx](#)
- [Bearbeiten einer Regex-Übereinstimmungsbedingung](#)

Erstellen einer Regex-Übereinstimmungsbedingung

Wenn Sie Regex-Übereinstimmungsbedingungen erstellen, geben Sie Mustersätze an, die die Zeichenfolge (mit einem regulären Ausdruck) identifizieren, nach der Sie suchen möchten. Anschließend fügen Sie diese Mustersätze zu Filtern hinzu, die den Teil der Webanfragen angeben, den AWS WAF Classic auf diesen Mustersatz überprüfen soll, z. B. den URI oder die Abfragezeichenfolge.

Sie können einem einzelnen Mustersatz mehrere reguläre Ausdrücke hinzufügen. Wenn Sie dies tun, werden diese Ausdrücke mit einem OR kombiniert. Das heißt, eine Webanforderung stimmt mit dem Mustersatz überein, wenn der entsprechende Teil der Anforderung mit einem der aufgeführten Ausdrücke übereinstimmt.

Wenn Sie einer Regel eine Regex-Übereinstimmungsbedingung hinzufügen, können Sie AWS WAF Classic auch so konfigurieren, dass Webanfragen zugelassen oder blockiert werden, die nicht den Werten in der Bedingung entsprechen.

AWS WAF Classic unterstützt die meisten [standardmäßigen Perl-kompatiblen regulären Ausdrücke \(PCRE\)](#). Folgende Transaktionen werden allerdings nicht unterstützt:

- Rückverweise und Erfassung von Teilausdrücken
- Willkürliche Null-Breite-Assertionen
- Subroutine-Referenzen und rekursive Muster
- Bedingungsmuster
- Rückverfolgung von Kontrollverben
- Die \C Einbyte-Richtlinie

- Die \ R-Newline-Match-Richtlinie
- Die \ K-Start der Match-Reset-Richtlinie
- Callouts und eingebetteter Code
- Atomic Grouping und possessive Quantifizierer

So erstellen Sie eine Regex-Übereinstimmungsbedingung

1. [Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter https://console.aws.amazon.com/wafv2/.](https://console.aws.amazon.com/wafv2/)

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich String and regex matching aus.
3. Wählen Sie Create condition.
4. Geben Sie die entsprechenden Filtereinstellungen an. Weitere Informationen finden Sie unter [Werte, die Sie angeben, wenn Sie Abgleichsbedingungen erstellen oder bearbeiten RegEx](#).
5. Wählen Sie Create pattern set and add filter (wenn Sie einen neuen Mustersatz erstellt haben) oder Add filter, wenn Sie einen vorhandenen Mustersatz verwendet haben.
6. Wählen Sie Erstellen.

Werte, die Sie angeben, wenn Sie Abgleichsbedingungen erstellen oder bearbeiten RegEx

Beim Erstellen oder Aktualisieren einer Regex-Übereinstimmungsbedingung geben Sie die folgenden Werte an:

Name

Geben Sie einen Namen für die regex-Abgleichsbedingung ein. Der Name darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) oder die folgenden Sonderzeichen enthalten: `_! "#` +*},./`. Sie können den Namen einer Bedingung nicht mehr ändern, nachdem Sie sie erstellt haben.

Typ

Wählen Sie Regex match

Teil der Anforderung, nach dem gefiltert werden soll

Wählen Sie den Teil jeder Webanforderung aus, den AWS WAF Classic auf das Muster überprüfen soll, das Sie unter Zuordnender Wert angegeben haben:

Header

Ein angegebener Anforderungs-Header, wie z. B. der `User-Agent`- oder `Referer`-Header. Wenn Sie Header auswählen, geben Sie den Namen des Headers im Feld Header an.

HTTP-Methode

Die HTTP-Methode, die den Typ des Vorgangs angibt, den die Anfrage vom Ursprung ausführen soll. CloudFront unterstützt die folgenden Methoden: `DELETE`, `GET`, `HEAD`, `OPTIONS`, `PATCH`, `POST`, und `PUT`.

Abfragezeichenfolge

Der Teil einer URL nach einem `?`-Zeichen, sofern vorhanden.

URI

Der URI-Pfad der Anfrage, der die Ressource identifiziert, `/images/daily-ad.jpg` z. B. Dies beinhaltet nicht die Abfragezeichenfolge oder die Fragmentkomponenten der URI. Informationen dazu finden Sie unter [Uniform Resource Identifier \(URI\): Generic Syntax](#).

Sofern keine Transformation angegeben ist, ist ein URI nicht normalisiert und wird genauso geprüft, wie er im Rahmen der Anfrage vom Client AWS empfangen wird. Eine Transformation formatiert die URI wie vorgegeben neu.

Fließtext

Der Teil einer Anforderung, der zusätzliche Daten enthält, die Sie als HTTP-Anforderungstext an Ihren Webserver senden möchten, wie z. B. Formulardaten.

Note

Wenn Sie für den Wert Teil der Anforderung, nach dem gefiltert werden soll, `Body` wählen, untersucht AWS WAF Classic nur die ersten 8192 Byte (8 KB). Um Anfragen zuzulassen oder zu blockieren, deren Hauptteil länger als 8192 Byte ist, können Sie eine Größenbeschränkungsbedingung erstellen. (AWS WAF Classic ermittelt die Länge des Hauptteils aus den Anforderungsheadern.) Weitere Informationen finden Sie unter [Arbeiten mit Größenbeschränkungsbedingungen](#).

Einzelner Abfrageparameter (ausschließlich Wert)

Jeder Parameter, den Sie als Teil der Abfragezeichenfolge definiert haben. Wenn die URL beispielsweise „www.xyz.com? UserName =abc& SalesRegion =seattle“ lautet, können Sie entweder dem Parameter oder einen Filter hinzufügen. `UserNameSalesRegion`

Wenn doppelte Parameter in der Abfragezeichenfolge enthalten sind, werden die Werte als "ODER" gewertet. Das heißt, dass auch nur einer der Werte ausreicht, um eine Übereinstimmung auszulösen. Beispiel: In der URL „www.xyz.com? SalesRegion =boston& SalesRegion =seattle“ löst ein Muster, das entweder mit „Boston“ oder „Seattle“ im Wert „Übereinstimmender Wert“ übereinstimmt, einen Treffer aus.

Wenn Sie Einzelner Abfrageparameter (ausschließlich Wert) auswählen, legen Sie auch einen Abfrageparameternamen fest. Dies ist der Parameter in der Abfragezeichenfolge, den Sie überprüfen werden, z. B. `UserNameSalesRegion`. Die maximale Länge für den Abfrageparameternamen beträgt 30 Zeichen. Der Abfrageparametername berücksichtigt keine Groß- und Kleinschreibung. Wenn Sie beispielsweise den Namen des Query-Parameters angeben `UserName`, entspricht dies allen Varianten von `UserName`, z. B. `UsERName` und `userName`.

Alle Abfrageparameter (ausschließlich Werte)

Ähnlich wie Einzelner Abfrageparameter (nur Wert), untersucht AWS WAF Classic jedoch nicht den Wert eines einzelnen Parameters, sondern den Wert aller Parameter innerhalb der Abfragezeichenfolge auf das Muster, das im Feld Passender Wert angegeben ist.

Beispiel: In der URL „www.xyz.com? UserName =abc& SalesRegion =seattle“ ein Muster in Value to match, das entweder dem Wert in entspricht oder einen Treffer auslöst.

`UserNameSalesRegion`

Header (nur wenn "Teil der Filter" auf "Header" festgelegt ist)

Wenn Sie in der Liste „Teil der Anforderung, nach der gefiltert werden soll“ die Option „Kopfzeile“ ausgewählt haben, wählen Sie eine Kopfzeile aus der Liste der allgemeinen Kopfzeilen aus, oder geben Sie den Namen einer Kopfzeile ein, die Classic untersuchen soll. AWS WAF

Transformation

Eine Transformation formatiert eine Webanforderung neu, bevor AWS WAF Classic die Anfrage überprüft. Dadurch werden einige der ungewöhnlichen Formatierungen vermieden, die Angreifer in Webanfragen verwenden, um Classic zu umgehen AWS WAF .

Sie können nur einen einzigen Texttransformationstyp angeben.

Transformationen können die folgenden Vorgänge ausführen:

None

AWS WAF Classic führt keine Texttransformationen an der Webanforderung durch, bevor überprüft wird, ob die Zeichenfolge in Value übereinstimmt.

In Kleinbuchstaben konvertieren

AWS WAF Classic konvertiert Großbuchstaben (A-Z) in Kleinbuchstaben (a-z).

HTML-Dekodierung

AWS WAF Classic ersetzt HTML-kodierte Zeichen durch unkodierte Zeichen:

- Ersetzt `"` durch `&`
- Ersetzt ` ` durch ein geschütztes Leerzeichen
- Ersetzt `&l t;` durch `<`
- Ersetzt `>` durch `>`
- Ersetzt Zeichen im Hexadezimalformat `&#xhhhh;` mit dem entsprechenden Zeichen
- Ersetzt Zeichen im Dezimalformat `&#nnnn;` mit dem entsprechenden Zeichen

Leerzeichen normalisieren

AWS WAF Classic ersetzt die folgenden Zeichen durch ein Leerzeichen (Dezimalzahl 32):

- `\f`, Zeilenvorschubzeichen, Dezimalzahl 12
- `\t`, Tabulator, Dezimalzahl 9
- `\n`, Zeilenumbruch, Dezimalzahl 10
- `\r`, Wagenrücklauf, Dezimalzahl 13
- `\v`, vertikaler Tabulator, Dezimalzahl 11
- geschütztes Leerzeichen, Dezimalzahl 160

Diese Option ersetzt mehrere aufeinanderfolgende Leerzeichen durch 1 Leerzeichen.

Vereinfachen der Befehlszeile

Wenn Sie befürchten, dass Angreifer einen Befehlszeilen-Befehl des Betriebssystems einfügen und diesen Befehl ganz oder teilweise durch ungewöhnliche Formatierungen verbergen, verwenden Sie diese Option, um folgende Transformationen auszuführen:

- Löschen der folgenden Zeichen: \ " ' ^
- Löschen von Leerzeichen vor den folgenden Zeichen: / (
- Ersetzen der folgenden Zeichen durch ein Leerzeichen: , ;
- Ersetzen mehrerer Leerzeichen durch ein Leerzeichen
- Konvertieren von Groß- (A-Z) in Kleinbuchstaben (a-z)

URL-Dekodierung

Dekodieren Sie eine URL-kodierte Anforderung.

Regex-Muster zur Übereinstimmung mit der Anfrage

Sie können einen bestehenden Mustersatz auswählen oder einen neuen erstellen. Wenn Sie einen neuen erstellen, geben Sie Folgendes an:

Neuer Mustersatzname

Geben Sie einen Namen ein und geben Sie dann das Regex-Muster an, nach dem AWS WAF Classic suchen soll.

Wenn Sie einem Mustersatz mehrere reguläre Ausdrücke hinzufügen, werden diese Ausdrücke mit einem OR kombiniert. Das heißt, eine Webanforderung stimmt mit dem Mustersatz überein, wenn der entsprechende Teil der Anforderung mit einem der aufgeführten Ausdrücke übereinstimmt.


Die maximale Länge von Value to match ist 70 Zeichen.

Bearbeiten einer Regex-Übereinstimmungsbedingung

Sie können die folgenden Änderungen an einer vorhandenen Regex-Übereinstimmungsbedingung vornehmen:

- Löschen eines Musters aus einem vorhandenen Mustersatz
- Hinzufügen eines Musters zu einem vorhandenen Mustersatz
- Löschen eines Filters zu einer bestehenden Regex-Abgleichsbedingung
- Fügen Sie einer vorhandenen Regex-Übereinstimmungsbedingung einen Filter hinzu (Sie können nur einen Filter in einer Regex-Übereinstimmungsbedingung verwenden. Um einen Filter hinzuzufügen, müssen Sie daher zuerst den vorhandenen Filter löschen.)

- Löschen einer bestehenden Regex-Abgleichsbedingung

 Note

Sie können ein Mustersatz nicht aus einem vorhandenen Filter hinzufügen oder löschen. Sie müssen entweder den Mustersatz festlegen, bearbeiten oder löschen und einen neuen Filter mit einem neuen Mustersatz festlegen.

Löschen eines Musters aus einem vorhandenen Mustersatz

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich String and regex matching aus.
3. Wählen Sie View regex pattern sets.
4. Klicken Sie auf den Namen des Mustersatzs, den Sie durchsuchen möchten.
5. Wählen Sie Bearbeiten aus.
6. Wählen Sie X neben dem Muster, das Sie löschen möchten.
7. Wählen Sie Speichern.

Hinzufügen eines Musters zu einem vorhandenen Mustersatz

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich String and regex matching aus.
3. Wählen Sie View regex pattern sets.
4. Klicken Sie auf den Namen des Mustersatzs, den Sie bearbeiten möchten.
5. Wählen Sie Bearbeiten aus.
6. Geben Sie ein neues RegEx-Muster ein.

7. Wählen Sie die + neben dem neuen Muster.
8. Wählen Sie Speichern.

Löschen eines Filters in einer vorhandenen Regex-Übereinstimmungsbedingung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich String and regex matching aus.
3. Klicken Sie auf den Namen der Bedingung mit dem Filter, die Sie löschen möchten.
4. Wählen Sie das Kontrollkästchen neben dem Filter aus, den Sie löschen möchten.
5. Wählen Sie Delete filter.

So löschen Sie eine Regex-Übereinstimmungsbedingung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Löschen Sie den Filter aus der Regex-Bedingung. Anweisungen dazu finden Sie unter [Löschen eines Filters in einer vorhandenen Regex-Übereinstimmungsbedingung.](#))
3. Entfernen Sie die Regex-Übereinstimmungsbedingung aus den Regeln, die sie verwenden:
 - a. Wählen Sie im Navigationsbereich Regeln aus.
 - b. Wählen Sie den Namen einer Regel aus, die die Regex-Übereinstimmungsbedingung verwendet, die Sie löschen möchten.
 - c. Wählen Sie im rechten Bereich die Registerkarte Edit rule aus.
 - d. Wählen Sie X neben der Bedingung, die Sie löschen möchten.
 - e. Wählen Sie Aktualisieren.
 - f. Wiederholen Sie dies für alle übrigen Regeln, die die Regex-Übereinstimmungsbedingung verwenden, die Sie löschen möchten.
4. Wählen Sie im Navigationsbereich String and regex matching aus.

5. Wählen Sie die Schaltfläche neben der Bedingung, die Sie löschen möchten.
6. Wählen Sie Löschen aus.

So fügen Sie einen Filter zu einer vorhandenen Regex-Übereinstimmungsbedingung hinzu oder ändern ihn

Sie können nur einen Filter in einer Regex-Übereinstimmungsbedingung haben. Um einen Filter hinzuzufügen oder zu ändern, müssen Sie daher zuerst den vorhandenen Filter löschen.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Löschen Sie den Filter aus der Regex-Bedingung, die Sie ändern möchten. Anweisungen dazu finden Sie unter [Löschen eines Filters in einer vorhandenen Regex-Übereinstimmungsbedingung.](#))
3. Wählen Sie im Navigationsbereich String and regex matching aus.
4. Klicken Sie auf den Namen des Mustersatzes, den Sie durchsuchen möchten.
5. Wählen Sie Add filter.
6. Geben Sie die entsprechenden Werte für den neuen Filter ein und wählen Sie Add.

Arbeiten mit Regeln

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter. [AWS WAF](#)

Mit Regeln können Sie gezielt auf die Webanfragen abzielen, die AWS WAF Classic zulassen oder blockieren soll, indem Sie genau die Bedingungen angeben, auf die AWS WAF Classic achten soll.

AWS WAF Classic kann beispielsweise darauf achten, von welchen IP-Adressen Anfragen stammen, welche Zeichenfolgen die Anfragen enthalten und wo die Zeichenfolgen vorkommen und ob die Anfragen böstigen SQL-Code zu enthalten scheinen.

Themen

- [Erstellen einer Regel und Hinzufügen von Bedingungen](#)
- [Hinzufügen und Entfernen von Bedingungen in einer Regel](#)
- [Löschen einer Regel](#)
- [AWS Marketplace Regelgruppen](#)

Erstellen einer Regel und Hinzufügen von Bedingungen

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Wenn Sie einer Regel mehr als eine Bedingung hinzufügen, muss eine Webanforderung alle Bedingungen erfüllen, damit AWS WAF Classic Anfragen, die auf dieser Regel basieren, zulässt oder blockiert.

So erstellen Sie eine Regel und fügen Bedingungen hinzu

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich Rules aus.
3. Wählen Sie Regel erstellen aus.
4. Geben Sie die folgenden Werte ein:

Name

Geben Sie einen Namen ein.

CloudWatch Name der Metrik

Geben Sie einen Namen für die CloudWatch Metrik ein, die AWS WAF Classic erstellen und der Regel zuordnen wird. Der Name darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) mit höchstens 128 und mindestens einem Zeichen enthalten. Er darf keine Leerzeichen oder Metrikenamen enthalten, die für AWS WAF Classic reserviert sind, einschließlich „All“ und „Default_Action“.

Regeltyp

Wählen Sie `Regular rule` oder `Rate-based rule`. Ratenbasierte Regeln sind identisch mit regulären Regeln, berücksichtigen aber auch, wie viele Anfragen von einer IP-Adresse innerhalb von fünf Minuten eingehen. Weitere Informationen zu diesen Arten von Regeln finden Sie unter [So funktioniert AWS WAF Classic](#).

Ratenlimit

Geben Sie bei einer ratenbasierten Regel die maximale Anzahl von Anfragen ein, die in einem Zeitraum von fünf Minuten von einer IP-Adresse, die den Bedingungen der Regel entspricht, zulässig sind. Das Ratenlimit muss mindestens 100 betragen.

Sie können ein Ratenlimit allein oder ein Ratenlimit und Konditionen angeben. Wenn Sie nur ein Ratenlimit angeben, wird das AWS WAF Limit auf alle IP-Adressen angewendet. Wenn Sie ein Ratenlimit und Bedingungen angeben, AWS WAF wird das Limit auf IP-Adressen festgelegt, die den Bedingungen entsprechen.

Wenn eine IP-Adresse den Schwellenwert für die Ratenbegrenzung erreicht, wird die zugewiesene Aktion (Blockieren oder Zählen) so schnell wie möglich AWS WAF angewendet, normalerweise innerhalb von 30 Sekunden. Sobald die Aktion ausgeführt wurde und fünf Minuten ohne Anfragen von der IP-Adresse vergangen sind, AWS WAF wird der Zähler auf Null zurückgesetzt.

5. Wenn Sie der Regel eine Bedingung hinzufügen möchten, geben Sie die folgenden Werte an:

Eine Anforderung entspricht/entspricht nicht

Wenn Sie möchten, dass AWS WAF Classic Anfragen auf der Grundlage der Filter in einer Bedingung zulässt oder blockiert, wählen Sie „`tut`“. Wenn eine IP-

Übereinstimmungsbedingung beispielsweise den IP-Adressbereich 192.0.2.0/24 umfasst und Sie möchten, dass AWS WAF Classic Anfragen, die von diesen IP-Adressen kommen, zulässt oder blockiert, wählen Sie tut.

Wenn AWS WAF Classic Anfragen zulassen oder blockieren soll, die auf der Umkehrung der Filter in einer Bedingung basieren, wählen Sie „Nicht“. Wenn eine IP-Übereinstimmungsbedingung beispielsweise den IP-Adressbereich 192.0.2.0/24 umfasst und Sie möchten, dass AWS WAF Classic Anfragen zulässt oder blockiert, die nicht von diesen IP-Adressen stammen, wählen Sie „Nicht“.

übereinstimmen mit/stammen von

Wählen Sie die Art der Bedingung aus, die Sie der Regel hinzufügen möchten:

- Siteübergreifende Scripting-Übereinstimmungsbedingungen — Wählen Sie, ob mindestens einem der Filter in der Abgleichsbedingung für standortübergreifendes Scripting entsprechen muss
- IP-Übereinstimmungsbedingungen — wählen Sie, ob sie von einer IP-Adresse stammen aus
- Geo-Match-Bedingungen — wählen Sie aus, dass sie von einem geografischen Standort stammen in
- Bedingungen für Größenbeschränkungen — Wählen Sie, ob mindestens einer der Filter in der Größenbeschränkungsbedingung entspricht
- Übereinstimmungsbedingungen für SQL-Injection — Wählen Sie aus, ob mindestens einer der Filter in der SQL-Injection-Abgleichsbedingung entspricht
- Bedingungen für den Abgleich von Zeichenketten — wählen Sie, ob mindestens einer der Filter in der Bedingung für die Übereinstimmung mit Zeichenketten übereinstimmt
- Übereinstimmungsbedingungen für reguläre Ausdrücke — wählen Sie, ob mindestens einem der Filter in der Regex-Abgleichsbedingung entspricht

Bedingungsname

Wählen Sie die Bedingung aus, die Sie der Regel hinzufügen möchten. Die Liste enthält nur Bedingungen des Typs, den Sie im vorherigen Schritt ausgewählt haben.

6. Um der Regel eine andere Bedingung hinzufügen, wählen Sie Add another condition, und wiederholen Sie die Schritte 4 und 5. Beachten Sie Folgendes:

- Wenn Sie mehr als eine Bedingung hinzufügen, muss eine Webanforderung mindestens einem Filter in jeder Bedingung entsprechen, damit AWS WAF Classic Anfragen, die auf dieser Regel basieren, zulässt oder blockiert
 - Wenn Sie derselben Regel zwei IP-Übereinstimmungsbedingungen hinzufügen, erlaubt oder blockiert AWS WAF Classic nur Anfragen, die von IP-Adressen stammen, die in beiden IP-Übereinstimmungsbedingungen vorkommen
7. Wählen Sie nach dem Hinzufügen der Bedingungen Erstellen aus.

Hinzufügen und Entfernen von Bedingungen in einer Regel

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Sie können eine Regel ändern, indem Sie Bedingungen hinzufügen oder entfernen.

So fügen Sie Bedingungen in einer Regel hinzu oder entfernen sie

1. Melden Sie sich unter <https://console.aws.amazon.com/wafv2/> bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich Regeln aus.
3. Wählen Sie den Namen der Regel aus, in der Sie Bedingungen hinzufügen oder entfernen möchten.
4. Wählen Sie Regel hinzufügen aus.
5. Wenn Sie eine Bedingung hinzufügen möchten, wählen Sie Add condition, aus und geben Sie die folgenden Werte an:

Eine Anforderung entspricht/entspricht nicht

Wenn Sie möchten, dass AWS WAF Classic Anfragen basierend auf den Filtern in einer Bedingung zulässt oder blockiert, z. B. Webanfragen, die aus dem IP-Adressbereich 192.0.2.0/24 stammen, wählen Sie tut aus.

Wenn AWS WAF Classic Anfragen zulassen oder blockieren soll, die auf der Umkehrung der Filter in einer Bedingung basieren, wählen Sie „Nicht“. Wenn eine IP-Übereinstimmungsbedingung beispielsweise den IP-Adressbereich 192.0.2.0/24 umfasst und Sie möchten, dass AWS WAF Classic Anfragen zulässt oder blockiert, die nicht von diesen IP-Adressen stammen, wählen Sie „Nicht“.

übereinstimmen mit/stammen von

Wählen Sie die Art der Bedingung aus, die Sie der Regel hinzufügen möchten:

- Siteübergreifende Scripting-Übereinstimmungsbedingungen — Wählen Sie, ob mindestens einem der Filter in der Abgleichsbedingung für standortübergreifendes Scripting entsprechen muss
- IP-Übereinstimmungsbedingungen — wählen Sie, ob sie von einer IP-Adresse stammen aus
- Geo-Match-Bedingungen — wählen Sie aus, dass sie von einem geografischen Standort stammen in
- Bedingungen für Größenbeschränkungen — Wählen Sie, ob mindestens einer der Filter in der Größenbeschränkungsbedingung entspricht
- Übereinstimmungsbedingungen für SQL-Injection — wählen Sie, ob mindestens einer der Filter in der SQL-Injection-Abgleichsbedingung entspricht
- Bedingungen für den Abgleich von Zeichenketten — wählen Sie, ob mindestens einer der Filter in der Bedingung für die Übereinstimmung mit Zeichenketten übereinstimmt
- Übereinstimmungsbedingungen für reguläre Ausdrücke — wählen Sie, ob mindestens einem der Filter in der Regex-Abgleichsbedingung entspricht

Bedingungsname

Wählen Sie die Bedingung aus, die Sie der Regel hinzufügen möchten. Die Liste enthält nur Bedingungen des Typs, den Sie im vorherigen Schritt ausgewählt haben.

6. Um eine Bedingung zu entfernen, wählen Sie das X rechts neben dem Bedingungsnamen
7. Wählen Sie Aktualisieren.

Löschen einer Regel

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Wenn Sie eine Regel löschen möchten, müssen Sie sie zuerst aus den Web-ACLs entfernen, von denen sie verwendet wird, und anschließend die Bedingungen löschen, die in der Regel enthalten sind.

So löschen Sie eine Regel

1. Melden Sie sich unter <https://console.aws.amazon.com/wafv2/> bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Um die Regel aus den Web-ACLs zu entfernen, die sie verwenden, führen Sie die folgenden Schritte für jede der Web-ACLs aus:
 - a. Wählen Sie im Navigationsbereich Web ACLs aus.
 - b. Wählen Sie den Namen einer Web-ACL aus, von der die Regel, die Sie löschen möchten, verwendet wird.
 - c. Wählen Sie die Registerkarte Rules (Regeln).
 - d. Wählen Sie Edit Web ACL aus.
 - e. Wählen Sie das X rechts neben der Regel aus, die Sie löschen möchten, und wählen Sie dann Aktualisieren aus.
3. Wählen Sie im Navigationsbereich Regeln aus.
4. Wählen Sie den Namen der Regel aus, die Sie löschen möchten.
5. Wählen Sie Löschen.

AWS Marketplace Regelgruppen

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

AWS WAF Classic bietet AWS Marketplace Regelgruppen, mit denen Sie Ihre Ressourcen schützen können. AWS Marketplace Regelgruppen sind Sammlungen vordefinierter ready-to-use Regeln, die von AWS Partnerunternehmen geschrieben AWS und aktualisiert wurden.

Einige AWS Marketplace Regelgruppen wurden entwickelt, um bestimmte Arten von Webanwendungen wie WordPress Joomla oder PHP zu schützen. Andere AWS Marketplace Regelgruppen bieten umfassenden Schutz vor bekannten Bedrohungen oder häufigen Sicherheitslücken in Webanwendungen, wie sie beispielsweise in den [OWASP](#) Top 10 aufgeführt sind.

Sie können eine einzelne AWS Marketplace Regelgruppe von Ihrem bevorzugten AWS Partner installieren, und Sie können auch Ihre eigenen, benutzerdefinierten AWS WAF Classic-Regeln hinzufügen, um den Schutz zu erhöhen. Wenn Sie behördlichen Auflagen wie PCI oder HIPAA unterliegen, können Sie möglicherweise AWS Marketplace Regelgruppen verwenden, um die Firewall-Anforderungen für Webanwendungen zu erfüllen.

AWS Marketplace Regelgruppen sind ohne langfristige Verträge und ohne Mindestverpflichtungen erhältlich. Wenn Sie eine Regelgruppe abonnieren, werden Ihnen monatliche Gebühren (auf Stunden umgelegt) und kontinuierliche Gebühren für Anforderungen nach Volumen berechnet. Weitere Informationen finden Sie unter [AWS WAF Klassische Preisgestaltung](#) und in der Beschreibung der einzelnen AWS Marketplace Regelgruppen unter AWS Marketplace.

Automatische Updates

Es kann zeitaufwändig und teuer sein, sich über die sich ständig ändernde Bedrohungslandschaft auf dem Laufenden zu halten. AWS Marketplace Regelgruppen können Ihnen bei der Implementierung und Verwendung von AWS WAF Classic Zeit sparen. Ein weiterer Vorteil besteht darin, dass AWS

unsere AWS Partner AWS Marketplace Regelgruppen automatisch aktualisieren, wenn neue Sicherheitslücken und Bedrohungen auftauchen.

Viele unserer Partner werden vor der Veröffentlichung über neue Schwachstellen informiert. Sie können ihre Regelgruppen aktualisieren und sie für Sie bereitstellen, bevor eine neue Bedrohung weithin bekannt ist. Viele von ihnen haben auch Teams für die Erforschung von Bedrohungen und die Analyse der neuesten Bedrohungen, um die relevantesten Regeln zu schreiben.

Zugriff auf die Regeln in einer AWS Marketplace Regelgruppe

Jede AWS Marketplace Regelgruppe bietet eine umfassende Beschreibung der Arten von Angriffen und Sicherheitslücken, vor denen sie schützen soll. Um das geistige Eigentum der Regelgruppenanbieter zu schützen, können Sie die einzelnen Regeln nicht innerhalb einer Regelgruppe anzeigen. Diese Einschränkung hilft auch, böswillige Benutzer daran zu hindern, Bedrohungen zu entwerfen, die speziell veröffentlichte Regeln umgehen.

Da Sie einzelne Regeln in einer AWS Marketplace Regelgruppe nicht anzeigen können, können Sie auch keine Regeln in einer AWS Marketplace Regelgruppe bearbeiten. Sie können jedoch spezifische Regeln aus einer Regelgruppe ausschließen. Dies wird als „Regelgruppenausnahme“ bezeichnet. Durch den Ausschluss werden die betreffenden Regeln nicht entfernt. Stattdessen wird die Aktion für die Regeln auf COUNT festgelegt. Anforderungen, die mit einer ausgeschlossenen Regel übereinstimmen, werden daher gezählt, aber nicht blockiert. Sie erhalten für jede ausgeschlossene Regel COUNT-Metriken.

Der Ausschluss von Regeln kann nützlich sein, wenn Sie Fehler für Regelgruppen beheben möchten, die den Datenverkehr unerwartet blockieren (falsch-positive Regeln). Eine Fehlerbehebungstechnik besteht in der Identifizierung der spezifischen Regel innerhalb der Regelgruppe, die den gewünschten Datenverkehr blockiert, und diese Regel anschließend zu deaktivieren (auszuschließen).

Zusätzlich zum Ausschluss spezifischer Regeln können Sie den Schutz optimieren, indem Sie ganze Regelgruppen aktivieren oder deaktivieren und die Regelgruppenaktion auswählen, die ausgeführt werden soll. Weitere Informationen finden Sie unter [AWS Marketplace Regelgruppen verwenden](#).

Kontingente

Sie können nur eine AWS Marketplace Regelgruppe aktivieren. Sie können auch eine benutzerdefinierte Regelgruppe aktivieren, mit der Sie erstellen AWS Firewall Manager. Diese Regelgruppen zählen für das maximale Kontingent von 10 Regeln pro Web-ACL. Daher können

Sie eine AWS Marketplace Regelgruppe, eine benutzerdefinierte Regelgruppe und bis zu acht benutzerdefinierte Regeln in einer einzigen Web-ACL haben.

Preisgestaltung

Die Preise für AWS Marketplace Regelgruppen finden Sie unter [AWS WAF Klassische Preisgestaltung](#) und in der Beschreibung AWS Marketplace der einzelnen Regelgruppen AWS Marketplace.

AWS Marketplace Regelgruppen verwenden

Sie können AWS Marketplace Regelgruppen auf der AWS WAF Classic-Konsole abonnieren und abbestellen. Sie können auch spezifische Regeln aus einer Regelgruppe ausschließen.

Um eine AWS Marketplace Regelgruppe zu abonnieren und zu verwenden

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich die Option Marketplace aus.
3. Wählen Sie im Abschnitt Available marketplace products den Namen einer Regelgruppe aus, um die Details und Preisinformationen anzuzeigen.
4. Wenn Sie die Regelgruppe abonnieren möchten, wählen Sie Continue.

Note

Wenn Sie diese Regelgruppe nicht abonnieren möchten, schließen Sie einfach diese Seite in Ihrem Browser.

5. Wählen Sie Set up your account.
6. Fügen Sie die Regelgruppe zu einer Web-ACL hinzu, so wie Sie eine einzelne Regel hinzufügen würden. Weitere Informationen finden Sie unter [Erstellen einer Web-ACL](#) oder [Bearbeiten einer Web-ACL](#).

Note

Wenn Sie einer Web-ACL eine Regelgruppe hinzufügen, wird die von Ihnen für die Regelgruppe festgelegte Aktion (No override (Keine Überschreibung) oder Override to count (Überschreiben für Zähler)) als Regelgruppen-Überschreibungsaktion bezeichnet. Weitere Informationen finden Sie unter [Überschreiben der Regelgruppe](#).

Um sich von einer AWS Marketplace Regelgruppe abzumelden

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Entfernen Sie die Regelgruppe aus allen Web-ACLs. Weitere Informationen finden Sie unter [Bearbeiten einer Web-ACL](#).
3. Wählen Sie im Navigationsbereich die Option Marketplace aus.
4. Wählen Sie Manage Your Subscriptions.
5. Wählen Sie Cancel subscription neben den Namen der Regelgruppe, die Sie kündigen möchten.
6. Wählen Sie Yes, cancel subscription.


So schließen Sie eine Regel aus einer Regelgruppe aus (Regelgruppenausnahme):

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Falls nicht bereits aktiviert, aktivieren Sie die AWS WAF klassische Protokollierung. Weitere Informationen finden Sie unter [Protokollieren von Web-ACL-Traffic-Informationen](#). Verwenden Sie die AWS WAF Classic-Protokolle, um die IDs der Regeln zu identifizieren, die Sie ausschließen möchten. Dies sind in der Regel Regeln, die legitime Anforderungen blockieren.
3. Wählen Sie im Navigationsbereich Web ACLs aus.


4. Wählen Sie den Namen der Web-ACL aus, die Sie bearbeiten möchten. Dadurch wird im rechten Bereich eine Seite mit den Details der Web-ACL geöffnet.

 Note

Die Regelgruppe, die Sie bearbeiten möchten, muss mit einer Web-ACL verknüpft sein, um eine Regel aus dieser Regelgruppe ausschließen zu können.

5. Wählen Sie auf der Registerkarte Rules im rechten Bereich Edit web ACL.
6. Erweitern Sie im Abschnitt Rule group exceptions (Regelgruppenausnahmen) die Regelgruppe, die Sie bearbeiten möchten.
7. Wählen Sie neben der Regel, die Sie ausschließen möchten, X aus. Sie können die richtige Regel-ID anhand der AWS WAF Classic-Protokolle ermitteln.
8. Wählen Sie Aktualisieren.

Durch den Ausschluss werden die betroffenen Regeln nicht aus der Regelgruppe entfernt. Stattdessen wird die Aktion für die Regeln auf COUNT festgelegt. Anforderungen, die mit einer ausgeschlossenen Regel übereinstimmen, werden daher gezählt, aber nicht blockiert. Sie erhalten für jede ausgeschlossene Regel COUNT-Metriken.

 Note

Sie können dieses Verfahren auch verwenden, um Regeln aus benutzerdefinierten Regelgruppen auszuschließen, die Sie in AWS Firewall Manager erstellt haben. Anstatt eine Regel auf diese Weise aus einer benutzerdefinierten Regelgruppe auszuschließen, können Sie eine benutzerdefinierte Regel auch einfach anhand der in [Hinzufügen und Löschen von Regeln aus einer AWS WAF klassischen Regelgruppe](#) beschriebenen Schritte bearbeiten.

Überschreiben der Regelgruppe

AWS Marketplace Für Regelgruppen gibt es zwei mögliche Aktionen: Kein Überschreiben und Überschreiben, um zu zählen. Wenn Sie die Regelgruppe testen möchten, setzen Sie die Aktion auf Override to count. Diese Regelgruppenaktion überschreibt alle Blockierungs-Aktionen, die von einzelnen Regeln innerhalb der Gruppe angegeben werden. Wenn also die Aktion der Regelgruppe auf Override to count gesetzt ist, statt potenziell übereinstimmende Anforderungen basierend auf

der Aktion einzelner Regeln innerhalb der Gruppe zu blockieren, werden diese Anforderungen erfasst. Wenn Sie dagegen die Aktion der Regelgruppe auf No override setzen, werden Aktionen der einzelnen Regeln innerhalb der Gruppe verwendet.

Fehlerbehebung bei AWS Marketplace -Regelgruppen

Wenn Sie feststellen, dass eine AWS Marketplace Regelgruppe legitimen Datenverkehr blockiert, führen Sie die folgenden Schritte aus.

So behandeln Sie Probleme mit einer AWS Marketplace -Regelgruppe

1. Schließen Sie die spezifischen Regeln aus, die legitimen Datenverkehr blockieren. Anhand der AWS WAF Classic-Protokolle können Sie feststellen, welche Regeln welche Anfragen blockieren. Weitere Informationen zum Ausschließen von Regeln finden Sie unter [So schließen Sie eine Regel aus einer Regelgruppe aus \(Regelgruppenausnahme\)](#):
2. Wenn das Problem durch das Ausschließen bestimmter Regeln nicht behoben werden kann, können Sie die Aktion für die AWS Marketplace Regelgruppe von „Keine Überschreibung“ in „Überschreiben“ ändern, um zu zählen. Dadurch kann die Webanforderung unabhängig von den einzelnen Regelaktionen innerhalb der Regelgruppe durchlaufen werden. Dadurch erhalten Sie auch CloudWatch Amazon-Metriken für die Regelgruppe.
3. Nachdem Sie die AWS Marketplace Regelgruppenaktion auf Override to count gesetzt haben, wenden Sie sich an das Kundenserviceteam des Regelgruppenanbieters, um das Problem weiter zu beheben. Kontaktinformationen finden Sie in der Regelgruppenliste auf den Produktlistenseiten auf AWS Marketplace.

Kontakt zum Kundenservice

Bei Problemen mit AWS WAF Classic oder einer Regelgruppe, die von verwaltet wird AWS, wenden Sie sich an AWS Support. Bei Problemen mit einer Regelgruppe, die von einem AWS Partner verwaltet wird, wenden Sie sich an das Kundensupport-Team dieses Partners. Kontaktinformationen für Partner finden Sie in der Liste des Partners unter AWS Marketplace.

AWS Marketplace Regelgruppen erstellen und verkaufen

Wenn Sie AWS Marketplace Regelgruppen weiterverkaufen möchten AWS Marketplace, finden Sie weitere Informationen unter [So verkaufen Sie Ihre Software weiter AWS Marketplace](#).

Arbeiten mit Web-ACLs

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Wenn Sie einer Web-ACL Regeln hinzufügen, geben Sie an, ob AWS WAF Classic Anfragen auf der Grundlage der Bedingungen in den Regeln zulassen oder blockieren soll. Wenn Sie einer Web-ACL mehr als eine Regel hinzufügen, bewertet AWS WAF Classic jede Anfrage anhand der Regeln in der Reihenfolge, in der Sie sie in der Web-ACL auflisten. Wenn eine Webanforderung alle Bedingungen in einer Regel erfüllt, führt AWS WAF Classic sofort die entsprechende Aktion aus — Zulassen oder Blockieren — und wertet die Anfrage nicht anhand der verbleibenden Regeln in der Web-ACL aus, falls vorhanden.

Wenn eine Webanforderung keiner der Regeln in einer Web-ACL entspricht, führt AWS WAF Classic die Standardaktion aus, die Sie für die Web-ACL angegeben haben. Weitere Informationen finden Sie unter [Bestimmen der Standardaktion für eine Web-ACL](#).

Wenn Sie eine Regel testen möchten, bevor Sie sie zum Zulassen oder Blockieren von Anfragen verwenden, können Sie AWS WAF Classic so konfigurieren, dass die Webanfragen gezählt werden, die den Bedingungen in der Regel entsprechen. Weitere Informationen finden Sie unter [Testen von Web-ACLs](#).

Themen

- [Bestimmen der Standardaktion für eine Web-ACL](#)
- [Erstellen einer Web-ACL](#)
- [Zuordnen oder Aufheben der Zuordnung einer Web-ACL zu einer Amazon API Gateway Gateway-API, einer CloudFront Distribution oder einem Application Load Balancer](#)
- [Bearbeiten einer Web-ACL](#)
- [Löschen einer Web-ACL](#)
- [Testen von Web-ACLs](#)

Bestimmen der Standardaktion für eine Web-ACL

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Wenn Sie eine Web-ACL erstellen und konfigurieren, müssen Sie zunächst entscheiden, ob die Standardaktion für AWS WAF Classic das Zulassen von Webanfragen oder das Blockieren von Webanfragen gelten soll. Die Standardaktion gibt an, was AWS WAF Classic tun soll, nachdem es eine Webanforderung auf alle von Ihnen angegebenen Bedingungen überprüft hat und die Webanforderung keiner dieser Bedingungen entspricht:

- **Zulassen** — Wenn Sie den meisten Benutzern den Zugriff auf Ihre Website ermöglichen möchten, Sie aber den Zugriff für Angreifer blockieren möchten, deren Anfragen von bestimmten IP-Adressen stammen oder deren Anfragen böartigen SQL-Code oder bestimmte Werte zu enthalten scheinen, wählen Sie Allow als Standardaktion aus.
- **Blockieren** — Wenn Sie verhindern möchten, dass die meisten potenziellen Benutzer auf Ihre Website zugreifen, Sie aber Benutzern Zugriff gewähren möchten, deren Anfragen von bestimmten IP-Adressen stammen oder deren Anfragen bestimmte Werte enthalten, wählen Sie Blockieren als Standardaktion.

Nachdem Sie eine Standardaktion ausgewählt haben, hängen viele Entscheidungen davon ab, ob Sie die meisten Webanforderungen zulassen oder blockieren möchten. Wenn Sie z. B. die meisten Anforderungen zulassen möchten, sollten Sie in den Übereinstimmungsbedingungen die Webanforderungen, die Sie blockieren möchten, generell angeben, z. B.:

- Anforderungen, die von IP-Adressen stammen, die eine übermäßige Anzahl von Anforderungen senden
- Anfragen, die aus Ländern stammen, in denen Sie keine Geschäfte tätigen oder die häufige Quelle von Angriffen sind
- Anforderungen mit gefälschten Werten im User-Agent-Header

- Anforderungen, die anscheinend schädlichen SQL-Code enthalten

Erstellen einer Web-ACL

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

So erstellen Sie eine Web-ACL

1. Melden Sie sich unter <https://console.aws.amazon.com/wafv2/> bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole.


Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wenn Sie AWS WAF Classic zum ersten Mal verwenden, wählen Sie Go to AWS WAF Classic und dann Configure Web ACL. Wenn Sie AWS WAF Classic schon einmal verwendet haben, wählen Sie im Navigationsbereich Web-ACLs und dann Web-ACL erstellen aus.
3. Geben Sie unter Web-ACL-Name einen Namen ein.

Note

Sie können den Namen nach dem Erstellen der Web-ACL nicht mehr ändern.

4. Ändern Sie für den CloudWatch Metrikenamen gegebenenfalls den Standardnamen. Der Name darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) mit höchstens 128 und mindestens einem Zeichen enthalten. Er darf keine Leerzeichen oder Metrikenamen enthalten, die für AWS WAF Classic reserviert sind, einschließlich „All“ und „Default_Action“.

 Note

Sie können den Namen nach dem Erstellen der Web-ACL nicht mehr ändern.

5. Wählen Sie unter -Region eine Region aus.
6. Wählen Sie für AWS resource die Ressource aus, die Sie mit dieser Web-ACL verknüpfen möchten, und dann Next.
7. Wenn Sie bereits die Bedingungen erstellt haben, die AWS WAF Classic zur Prüfung Ihrer Webanfragen verwenden soll, wählen Sie Weiter und fahren Sie dann mit dem nächsten Schritt fort.

Wenn Sie noch keine Bedingungen erstellt haben, holen Sie diesen Schritt jetzt nach. Weitere Informationen finden Sie unter den folgenden Themen:

- [Arbeiten mit Cross-Site-Scripting-Übereinstimmungsbedingungen](#)
- [Arbeiten mit IP-Übereinstimmungsbedingungen](#)
- [Arbeiten mit Geo-Übereinstimmungsbedingungen](#)
- [Arbeiten mit Größenbeschränkungsbedingungen](#)
- [Arbeiten mit SQL Injections-Übereinstimmungsbedingungen](#)
- [Arbeiten mit Zeichenfolgen-Übereinstimmungsbedingungen](#)
- [Arbeiten mit Regex-Übereinstimmungsbedingungen](#)

8. Wenn Sie die Regeln oder Regelgruppen, die Sie zu dieser Web-ACL hinzufügen möchten, bereits erstellt (oder eine AWS Marketplace Regelgruppe abonniert) haben, fügen Sie die Regeln der Web-ACL hinzu:
 - a. Wählen Sie eine Regel in der Rules-Liste aus.
 - b. Wählen Sie Add rule to web ACL.
 - c. Wiederholen Sie die Schritte a und b, bis Sie dieser Web-ACL alle gewünschten Regeln hinzugefügt haben.
 - d. Fahren Sie mit Schritt 10 fort.
9. Wenn Sie noch keine Regeln erstellt haben, können Sie jetzt Regeln hinzufügen:
 - a. Wählen Sie Regel erstellen aus.
 - b. Geben Sie die folgenden Werte ein:

Name

Geben Sie einen Namen ein.

CloudWatch Name der Metrik

Geben Sie einen Namen für die CloudWatch Metrik ein, die AWS WAF Classic erstellen und der Regel zuordnen wird. Der Name darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) mit höchstens 128 und mindestens einem Zeichen enthalten. Er darf keine Leerzeichen oder Metrikenamen enthalten, die für AWS WAF Classic reserviert sind, einschließlich „All“ und „Default_Action“.

Note

Sie können den Metrikenamen nach dem Erstellen der Regel nicht mehr ändern.

- c. Wenn Sie der Regel eine Bedingung hinzufügen möchten, geben Sie die folgenden Werte an:

Eine Anforderung entspricht/entspricht nicht

Wenn Sie möchten, dass AWS WAF Classic Anfragen, die auf den Filtern in einer Bedingung basieren, zulässt oder blockiert, z. B. Webanfragen, die aus dem IP-Adressbereich 192.0.2.0/24 stammen, wählen Sie **does**.

Wenn AWS WAF Classic Anfragen zulassen oder blockieren soll, die auf der Umkehrung der Filter in einer Bedingung basieren, wählen Sie **„Nicht“**. Wenn eine IP-Übereinstimmungsbedingung beispielsweise den IP-Adressbereich 192.0.2.0/24 umfasst und Sie möchten, dass AWS WAF Classic Anfragen zulässt oder blockiert, die nicht von diesen IP-Adressen stammen, wählen Sie **„Nicht“**.

übereinstimmen mit/stammen von

Wählen Sie die Art der Bedingung aus, die Sie der Regel hinzufügen möchten:

- Siteübergreifende Scripting-Übereinstimmungsbedingungen — Wählen Sie, ob mindestens einem der Filter in der Abgleichsbedingung für standortübergreifendes Scripting entsprechen muss
- IP-Übereinstimmungsbedingungen — wählen Sie, ob sie von einer IP-Adresse stammen aus

- Geo-Match-Bedingungen — wählen Sie aus, dass sie von einem geografischen Standort stammen in
- Größenbeschränkungsbedingungen — Wählen Sie aus, ob mindestens einer der Filter in der Größenbeschränkungsbedingung entspricht
- Übereinstimmungsbedingungen für SQL-Injection — Wählen Sie aus, ob mindestens einer der Filter in der SQL-Injection-Abgleichsbedingung entspricht
- Bedingungen für den Abgleich von Zeichenketten — wählen Sie, ob mindestens einer der Filter in der Bedingung für die Übereinstimmung mit Zeichenketten übereinstimmen muss
- Regex-Übereinstimmungsbedingungen — Wählen Sie aus, ob mindestens einer der Filter in der Regex-Abgleichsbedingung übereinstimmt

Bedingungsname

Wählen Sie die Bedingung aus, die Sie der Regel hinzufügen möchten. Die Liste enthält nur Bedingungen des Typs, den Sie in der vorherigen Liste ausgewählt haben.

- d. Wenn Sie der Regel eine weitere Bedingung hinzufügen möchten, wählen Sie Add another condition (Weitere Bedingung hinzufügen) aus und wiederholen Sie dann die Schritte b und c. Beachten Sie Folgendes:
 - Wenn Sie mehr als eine Bedingung hinzufügen, muss eine Webanforderung mindestens einem Filter in jeder Bedingung entsprechen, damit AWS WAF Classic Anfragen, die auf dieser Regel basieren, zulässt oder blockiert.
 - Wenn Sie derselben Regel zwei IP-Übereinstimmungsbedingungen hinzufügen, lässt AWS WAF Classic nur Anfragen zu oder blockiert, die von IP-Adressen stammen, die in beiden IP-Übereinstimmungsbedingungen vorkommen.
 - e. Wiederholen Sie Schritt 9, bis Sie alle Regeln für diese Web-ACL erstellt haben.
 - f. Wählen Sie Erstellen.
 - g. Fahren Sie mit Schritt 10 fort.
10. Wählen Sie für jede Regel oder Regelgruppe in der Web-ACL wie folgt die Art der Verwaltung aus, die AWS WAF Classic bereitstellen soll:
 - Wählen Sie für jede Regel anhand der Bedingungen in der Regel aus, ob AWS WAF Classic Webanfragen zulassen, blockieren oder zählen soll:

- **Zulassen** — API Gateway CloudFront oder ein Application Load Balancer antwortet mit dem angeforderten Objekt. Im Fall von CloudFront, wenn sich das Objekt nicht im Edge-Cache befindet, CloudFront leitet die Anfrage an den Ursprung weiter.
- **Blockieren** — API Gateway CloudFront oder ein Application Load Balancer antwortet auf die Anfrage mit einem HTTP-Statuscode 403 (Forbidden). CloudFront kann auch mit einer benutzerdefinierten Fehlerseite antworten. Weitere Informationen finden Sie unter [Verwenden von AWS WAF Classic mit CloudFront benutzerdefinierten Fehlerseiten](#).
- **Anzahl** — AWS WAF Classic erhöht einen Zähler von Anfragen, die den Bedingungen in der Regel entsprechen, und überprüft dann die Webanforderung auf der Grundlage der verbleibenden Regeln in der Web-ACL weiter.

Informationen darüber, wie Sie mit Count eine Web-ACL testen können, bevor Sie sie zum Zulassen oder Blockieren von Webanforderungen verwenden, finden Sie unter [Zählen der Webanforderungen, die den Regeln in einer Web-ACL entsprechen](#).

- Legen Sie für jede Regelgruppe die Überschreibungsaktion für die Regelgruppe fest:
 - **Keine Überschreibung** — Bewirkt, dass die Aktionen der einzelnen Regeln innerhalb der Regelgruppe verwendet werden.
 - **Überschreiben, um zu zählen** — Überschreibt alle Blockaktionen, die durch einzelne Regeln in der Gruppe spezifiziert sind, sodass nur alle übereinstimmenden Anfragen gezählt werden.

Weitere Informationen finden Sie unter [Überschreiben der Regelgruppe](#).

11. Wenn Sie die Reihenfolge der Regeln in der Web-ACL ändern möchten, verwenden Sie die Pfeile in der Spalte Reihenfolge. AWS WAF Classic überprüft Webanfragen anhand der Reihenfolge, in der Regeln in der Web-ACL erscheinen.
12. Wenn Sie eine Regel entfernen möchten, die Sie der Web-ACL hinzugefügt haben, wählen Sie x in der Zeile der Regel aus.
13. Wählen Sie die Standardaktion für die Web-ACL aus. Dies ist die Aktion, die AWS WAF Classic ergreift, wenn eine Webanforderung nicht den Bedingungen in einer der Regeln in dieser Web-ACL entspricht. Weitere Informationen finden Sie unter [Bestimmen der Standardaktion für eine Web-ACL](#).
14. Wählen Sie Review and create.
15. Überprüfen Sie die Einstellungen für die Web-ACL, und wählen Sie dann Confirm and create.

Zuordnen oder Aufheben der Zuordnung einer Web-ACL zu einer Amazon API Gateway Gateway-API, einer CloudFront Distribution oder einem Application Load Balancer

Note

Dies ist die Classic-Dokumentation.AWS WAF Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter. [AWS WAF](#)

Um eine Web-ACL zu verknüpfen oder zu trennen, führen Sie die entsprechenden Schritte aus. Beachten Sie, dass Sie einer CloudFront Distribution auch eine Web-ACL zuordnen können, wenn Sie die Distribution erstellen oder aktualisieren. Weitere Informationen finden Sie im Amazon CloudFront Developer Guide unter [Using AWS WAF Classic to Control Access to Your Content](#).

Die folgenden Einschränkungen gelten beim Zuordnen einer Web-ACL:

- Jede API Gateway Gateway-API, jeder Application Load Balancer und jede CloudFront Distribution kann nur einer Web-ACL zugeordnet werden.
- Mit einer CloudFront Distribution verknüpfte Web-ACLs können keiner Application Load Balancer- oder API Gateway zugeordnet werden. Die Web-ACL kann jedoch mit anderen CloudFront Distributionen verknüpft werden.

So verknüpfen Sie eine Web-ACL mit einer API Gateway Gateway-API, CloudFront Distribution oder einem Application Load Balancer

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich Web ACLs aus.

3. Wählen Sie den Namen der Web-ACL, die Sie einer API Gateway, CloudFront Distribution oder einem Application Load Balancer zuordnen möchten. Dadurch wird im rechten Bereich eine Seite mit den Details der Web-ACL geöffnet.
4. Wählen Sie auf der Registerkarte Regeln unter AWS Ressourcen, die diese Web-ACL verwenden, die Option Zuordnung hinzufügen aus.
5. Wenn Sie dazu aufgefordert werden, verwenden Sie die Ressourcenliste, um die API Gateway Gateway-API, CloudFront Distribution oder den Application Load Balancer auszuwählen, der Sie diese Web-ACL zuordnen möchten. Wenn Sie einen Application Load Balancer wählen, müssen Sie auch eine Region angeben.
6. Wählen Sie Hinzufügen aus.
7. Um diese Web-ACL mit einer zusätzlichen API Gateway Gateway-API, CloudFront Distribution oder einem anderen Application Load Balancer zu verknüpfen, wiederholen Sie die Schritte 4 bis 6.

So trennen Sie die Zuordnung einer Web-ACL zu einer API-Gateway-API, CloudFront Distribution oder einem Application Load Balancer

1. [Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter https://console.aws.amazon.com/wafv2/.](https://console.aws.amazon.com/wafv2/)

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich Web ACLs aus.
3. Wählen Sie den Namen der Web-ACL, die Sie von einer API Gateway, CloudFront Distribution oder einem Application Load Balancer trennen möchten. Dadurch wird im rechten Bereich eine Seite mit den Details der Web-ACL geöffnet.
4. Wählen Sie auf der Registerkarte Regeln unter AWS Ressourcen, die diese Web-ACL verwenden, das X für jede API-Gateway-API, CloudFront Distribution oder jeden Application Load Balancer aus, von dem Sie diese Web-ACL trennen möchten.

Bearbeiten einer Web-ACL

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Zum Hinzufügen oder Entfernen von Regeln aus einer Web-ACL oder zum Ändern der Standardaktion, gehen Sie wie folgt vor.


So bearbeiten Sie eine Web-ACL

1. Melden Sie sich unter <https://console.aws.amazon.com/wafv2/> bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich Web ACLs aus.
3. Wählen Sie den Namen der Web-ACL aus, die Sie bearbeiten möchten. Dadurch wird im rechten Bereich eine Seite mit den Details der Web-ACL geöffnet.
4. Wählen Sie auf der Registerkarte Rules im rechten Bereich Edit web ACL.
5. Um Regeln zur Web-ACL hinzuzufügen, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie in der Liste Rules die Regel aus, die Sie hinzufügen möchten.
 - b. Wählen Sie Add rule to web ACL.
 - c. Wiederholen Sie die Schritte a und b, bis Sie alle gewünschten Regeln hinzugefügt haben.
6. Wenn Sie die Reihenfolge der Regeln in der Web-ACL ändern möchten, verwenden Sie die Pfeile in der Spalte Reihenfolge. AWS WAF Classic überprüft Webanfragen anhand der Reihenfolge, in der Regeln in der Web-ACL erscheinen.
7. Um eine Regel aus der Web-ACL zu entfernen, wählen Sie auf der rechten Seite der Zeile mit der Regel x aus. Dadurch wird die Regel nicht aus AWS WAF Classic gelöscht, sondern sie wird lediglich aus dieser Web-ACL entfernt.


- Um die Aktion für eine Regel oder die Standardaktion für die Web-ACL zu ändern, wählen Sie die bevorzugte Option aus.

 Note

Wenn Sie die Aktion für eine Regelgruppe oder eine AWS Marketplace Regelgruppe (im Gegensatz zu einer einzelnen Regel) festlegen, wird die Aktion, die Sie für die Regelgruppe festlegen (entweder Keine Überschreibung oder Überschreiben, um zu zählen), als Überschreibungsaktion bezeichnet. Weitere Informationen finden Sie unter [Überschreiben der Regelgruppe](#)

- Wählen Sie Save Changes.

Löschen einer Web-ACL

 Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Um eine Web-ACL zu löschen, müssen Sie die Regeln entfernen, die in der Web-ACL enthalten sind, und alle CloudFront Distributionen und Application Load Balancer von der Web-ACL trennen. Führen Sie die folgenden Schritte aus.

So löschen Sie eine Web-ACL

- [Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter https://console.aws.amazon.com/wafv2/.](https://console.aws.amazon.com/wafv2/)

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

- Wählen Sie im Navigationsbereich Web ACLs aus.

3. Wählen Sie den Namen der Web-ACL, die Sie löschen möchten. Dadurch wird im rechten Bereich eine Seite mit den Details der Web-ACL geöffnet.
4. Wählen Sie auf der Registerkarte Rules im rechten Bereich Edit web ACL.
5. Um alle Regeln aus der Web-ACL zu entfernen, wählen Sie auf der rechten Seite der Zeile mit jeweiliger Regel x aus. Dadurch werden die Regeln nicht aus AWS WAF Classic gelöscht, sondern nur die Regeln aus dieser Web-ACL entfernt.
6. Wählen Sie Aktualisieren.
7. Trennen Sie die Web-ACL von allen CloudFront Distributionen und Application Load Balancern. Wählen Sie auf der Registerkarte Regeln unter AWS Ressourcen, die diese Web-ACL verwenden, das X für jede API-Gateway-API, CloudFront Distribution oder jeden Application Load Balancer aus.
8. Vergewissern Sie sich, dass die Web-ACL, die Sie löschen möchten, auf der Seite Web ACLs markiert ist und wählen Sie Delete (Löschen) aus.

Testen von Web-ACLs

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Um sicherzustellen, dass Sie AWS WAF Classic nicht versehentlich so konfigurieren, dass Webanfragen blockiert werden, die Sie zulassen möchten, oder Anfragen, die Sie blockieren möchten, zugelassen werden, empfehlen wir Ihnen, Ihre Web-ACL gründlich zu testen, bevor Sie sie auf Ihrer Website oder Webanwendung verwenden.

Themen

- [Zählen der Webanforderungen, die den Regeln in einer Web-ACL entsprechen](#)
- [Ein Beispiel der Webanfragen anzeigen, die API Gateway CloudFront oder ein Application Load Balancer an Classic weitergeleitet AWS WAF hat](#)

Zählen der Webanforderungen, die den Regeln in einer Web-ACL entsprechen

Wenn Sie einer Web-ACL Regeln hinzufügen, geben Sie an, ob AWS WAF Classic die Webanfragen zulassen, blockieren oder zählen soll, die alle Bedingungen in dieser Regel erfüllen. Wir empfehlen, mit der folgenden Konfiguration zu beginnen:

- Konfigurieren Sie alle Regeln in einer Web-ACL für das Zählen von Webanforderungen.
- Legen Sie als Standardaktion für die Web-ACL fest, dass Anforderungen zugelassen werden.

In dieser Konfiguration überprüft AWS WAF Classic jede Webanforderung auf der Grundlage der Bedingungen in der ersten Regel. Wenn die Webanforderung alle Bedingungen in dieser Regel erfüllt, erhöht AWS WAF Classic einen Zähler für diese Regel. Anschließend überprüft AWS WAF Classic die Webanforderung auf der Grundlage der Bedingungen in der nächsten Regel. Wenn die Anfrage alle Bedingungen in dieser Regel erfüllt, erhöht AWS WAF Classic einen Zähler für die Regel. Dies wird so lange fortgesetzt, bis AWS WAF Classic die Anfrage anhand der Bedingungen in all Ihren Regeln geprüft hat.

Nachdem Sie alle Regeln in einer Web-ACL zum Zählen von Anfragen konfiguriert und die Web-ACL mit einer Amazon API Gateway, CloudFront Distribution oder einem Application Load Balancer verknüpft haben, können Sie die resultierenden Zählungen in einem CloudWatch Amazon-Diagramm anzeigen. Für jede Regel in einer Web-ACL und für alle Anfragen, die API Gateway CloudFront oder ein Application Load Balancer für eine Web-ACL an AWS WAF Classic weiterleitet, CloudWatch können Sie:

- Anzeigen der Daten für die letzte Stunde oder für die letzten drei Stunden.
- Ändern der Intervalle zwischen Datenpunkten.
- Ändern Sie die Berechnung, CloudWatch die für die Daten ausgeführt wird, z. B. Maximum, Minimum, Durchschnitt oder Summe

Note

AWS WAF Classic with CloudFront ist ein globaler Service, und Metriken sind nur verfügbar, wenn Sie die Region USA Ost (Nord-Virginia) in der auswählen AWS Management Console. Wenn Sie eine andere Region wählen, werden keine AWS WAF Classic-Metriken in der CloudWatch Konsole angezeigt.

So zeigen Sie Daten für die Regeln in einer Web-ACL an

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie im Navigationsbereich unter Metrics die Option WAF aus.
3. Aktivieren Sie das Kontrollkästchen für die Web-ACL, für die Sie Daten anzeigen möchten.
4. Ändern Sie die geltenden Einstellungen:

Statistik

Wählen Sie die Berechnung CloudWatch aus, die mit den Daten durchgeführt wird.

Zeitraum

Wählen Sie aus, ob die Daten für die letzte Stunde oder für die letzten drei Stunden angezeigt werden sollen.

Intervall

Wählen Sie das Intervall zwischen den Datenpunkten in der Grafik aus.

Regeln

Wählen Sie die Regeln aus, für die Sie Daten anzeigen möchten.

Beachten Sie Folgendes:

- Wenn Sie gerade eine Web-ACL mit einer API Gateway Gateway-API, CloudFront Distribution oder einem Application Load Balancer verknüpft haben, müssen Sie möglicherweise einige Minuten warten, bis Daten im Diagramm und die Metrik für die Web-ACL in der Liste der verfügbaren Metriken angezeigt wird.
- Wenn Sie einer Web-ACL mehr als eine API Gateway Gateway-API, CloudFront Distribution oder Application Load Balancer zuordnen, enthalten die CloudWatch Daten alle Anfragen für alle Distributionen, die mit der Web-ACL verknüpft sind.
- Bewegen Sie den Cursor über einen Datenpunkt, um weitere Informationen zu erhalten.
- Die Grafik wird nicht automatisch aktualisiert. Wählen Sie zum Aktualisieren der Anzeige das Symbol



5. (Optional) Zeigen Sie detaillierte Informationen zu einzelnen Anfragen an, die API Gateway CloudFront oder ein Application Load Balancer an AWS WAF Classic weitergeleitet hat. Weitere Informationen finden Sie unter [Ein Beispiel der Webanfragen anzeigen, die API Gateway CloudFront oder ein Application Load Balancer an Classic weitergeleitet AWS WAF hat](#).
6. Falls Sie feststellen, dass eine Regel Anforderungen abfängt, die nicht abgefangen werden sollen, ändern Sie die geltenden Einstellungen. Weitere Informationen finden Sie unter [Erstellen und Konfigurieren einer Web-Zugriffskontrollliste \(Web-ACL\)](#).

Wenn alle Regeln nur die gewünschten Anforderungen abfangen und Sie zufrieden sind, ändern Sie die Aktion für die einzelnen Regeln zu Allow oder Block. Weitere Informationen finden Sie unter [Bearbeiten einer Web-ACL](#).

Ein Beispiel der Webanfragen anzeigen, die API Gateway CloudFront oder ein Application Load Balancer an Classic weitergeleitet AWS WAF hat

In der AWS WAF Classic-Konsole können Sie sich ein Beispiel der Anfragen ansehen, die API Gateway CloudFront oder ein Application Load Balancer zur Überprüfung an AWS WAF Classic weitergeleitet hat. Sie können zu jeder Anforderung in der Stichprobe detaillierte Daten aufrufen, z. B. die ursprüngliche IP-Adresse und die Header. Des Weiteren können Sie anzeigen, mit welcher Regel die Anforderung übereinstimmt und ob diese Regel zum Blockieren oder Zulassen von Anforderungen konfiguriert wurde.

Eine Stichprobe kann bis zu 100 Anforderungen enthalten, die allen Bedingungen in allen Regeln entsprechen, und weitere 100 Anforderungen für die Standardaktion, die für Anforderungen gilt, die nicht mit allen Bedingungen in allen Regeln übereinstimmen. Die Anfragen im Beispiel stammen von allen API Gateway Gateway-APIs, CloudFront Edge-Standorten oder Application Load Balancern, die in den letzten 15 Minuten Anfragen für Ihre Inhalte erhalten haben.

Um ein Beispiel der Webanfragen anzuzeigen, die API Gateway CloudFront oder ein Application Load Balancer an Classic weitergeleitet AWS WAF hat

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich die Web-ACL aus, für die Sie Anforderungen anzeigen möchten.

3. Wählen Sie im rechten Bereich die Registerkarte Requests aus.

In der Tabelle Sampled requests werden für jede Anforderung die folgenden Werte angegeben:

Quell-IP

Entweder die IP-Adresse, von der die Anforderung stammt, oder – falls das Anzeigeprogramm zum Senden der Anforderung einen HTTP-Proxy oder einen Application Load Balancer verwendet hat – die IP-Adresse des Proxys oder des Application Load Balancer.

URI

Der URI-Pfad der Anfrage, der die Ressource identifiziert, /images/daily-ad.jpg z. B. Dies beinhaltet nicht die Abfragezeichenfolge oder die Fragmentkomponenten der URI. Informationen dazu finden Sie unter [Uniform Resource Identifier \(URI\): Generic Syntax](#).

Regelübereinstimmung

Identifiziert die erste Regel der Web-ACL, bei der die Webanforderungen allen Bedingungen entspricht. Wenn eine Webanforderung nicht allen Bedingungen einer Regel der Web-ACL entspricht, wird für Matches rule der Wert Default verwendet.

Beachten Sie: Wenn eine Webanforderung alle Bedingungen in einer Regel erfüllt und die Aktion für diese Regel „Anzahl“ lautet, überprüft AWS WAF Classic die Webanforderung weiterhin auf der Grundlage der nachfolgenden Regeln in der Web-ACL. In diesem Fall kann eine Webanforderung zweimal in der Liste der per Stichprobe geprüften Anforderungen vorhanden sein: einmal für die Regel mit der Aktion Count und einmal für eine nachfolgende Regel bzw. für die Standardaktion.

Aktion

Gibt an, ob die Aktion für die entsprechende Regel Allow, Block oder Count lautet.

Zeit

Der Zeitpunkt, zu dem AWS WAF Classic die Anfrage von API Gateway CloudFront oder Ihrem Application Load Balancer erhalten hat.

4. Um zusätzliche Informationen zu der Anfrage anzuzeigen, wählen Sie den Pfeil auf der linken Seite der IP-Adresse für diese Anfrage. AWS WAF Classic zeigt die folgenden Informationen an:

Quell-IP

Die gleiche IP-Adresse wie in der Spalte Source IP in der Tabelle.

Land

Der zweistellige Ländercode des Landes, aus dem die Anforderung stammt. Falls das Anzeigeprogramm zum Senden der Anforderung ein HTTP-Proxy oder einen Application Load Balancer verwendet hat, ist dies der zweistellige Ländercode des Landes, in dem sich der HTTP-Proxy oder der Application Load Balancer befindet.

Eine Liste mit den zweistelligen Ländercodes und den zugehörigen Ländernamen finden Sie im Wikipedia-Eintrag [ISO 3166-1 alpha-2](#).

Methode

Die HTTP-Anforderungsmethode für die Anforderung: GET, HEAD, OPTIONS, PUT, POST, PATCH oder DELETE.

URI

Die gleiche URI wie in der Spalte URI in der Tabelle.

Anfordern von Headern

Die Anforderungs-Header und Header-Werte der Anforderung.

5. Um die Liste der Beispiele für Anforderungen zu aktualisieren, wählen Sie Get new samples.

Arbeiten mit AWS WAF klassischen Regelgruppen zur Verwendung mit AWS Firewall Manager

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Eine AWS WAF klassische Regelgruppe ist ein Regelsatz, den Sie zu einer AWS WAF AWS Firewall Manager Classic-Richtlinie hinzufügen. Sie können Ihre eigene Regelgruppe erstellen oder eine verwaltete Regelgruppe von erwerben AWS Marketplace.

Important

Wenn Sie Ihrer Firewall Manager Manager-Richtlinie eine AWS Marketplace Regelgruppe hinzufügen möchten, muss jedes Konto in Ihrer Organisation zuerst diese Regelgruppe abonnieren. Nachdem die Regelgruppe von allen Konten abonniert wurde, können Sie sie einer Richtlinie hinzufügen. Weitere Informationen finden Sie unter [AWS Marketplace Regelgruppen](#).

Themen

- [Eine AWS WAF klassische Regelgruppe erstellen](#)
- [Hinzufügen und Löschen von Regeln aus einer AWS WAF klassischen Regelgruppe](#)

Eine AWS WAF klassische Regelgruppe erstellen

Note


Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Wenn Sie eine AWS WAF klassische Regelgruppe für die Verwendung mit erstellen AWS Firewall Manager, geben Sie an, welche Regeln der Gruppe hinzugefügt werden sollen.


So erstellen Sie eine Regelgruppe (Konsole)

1. Melden Sie sich AWS Management Console mit dem AWS Firewall Manager Administratorkonto an, das Sie in den Voraussetzungen eingerichtet haben, und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fms>.

 Note


Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [Schritt 2: Erstellen Sie ein AWS Firewall Manager Standard-Administratorkonto](#).

2. Wählen Sie im Navigationsbereich die Option Zu AWS WAF Classic wechseln aus.
3. Wählen Sie im AWS WAF klassischen Navigationsbereich die Option Regelgruppen aus.
4. Wählen Sie Create rule group (Regelgruppe erstellen).

 Note

Sie können einer Regelgruppe keine ratenbasierten Regeln hinzufügen.

5. Wenn Sie die Regeln bereits erstellt haben, die Sie der Regelgruppe hinzufügen möchten, wählen Sie Use existing rules for this rule group (Vorhandene Regeln für diese Regelgruppe verwenden). Wenn Sie neue Regeln zum Hinzufügen zur Regelgruppe erstellen möchten, wählen Sie Create rules and conditions for this rule group (Regeln und Bedingungen für diese Regelgruppe erstellen).
6. Wählen Sie Weiter aus.
7. Wenn Sie sich für die Erstellung von Regeln entschieden haben, folgen Sie den Schritten zur Erstellung dieser Regeln in [Erstellen einer Regel und Hinzufügen von Bedingungen](#).

 Note

Verwenden Sie die AWS WAF Classic-Konsole, um Ihre Regeln zu erstellen.

Wenn Sie alle erforderlichen Regeln erstellt haben, fahren Sie mit dem nächsten Schritt fort.

8. Geben Sie einen Namen für die Regelgruppe ein.
9. Um eine Regel zur Regelgruppe hinzuzufügen, wählen Sie eine Regel und anschließend Add rule (Regel hinzufügen) aus. Wählen Sie aus, ob Anforderungen zugelassen, blockiert oder gezählt werden sollen, die mit den Bedingungen der Regel übereinstimmen. Weitere Informationen zu den Optionen finden Sie unter [So funktioniert AWS WAF Classic](#).
10. Wenn Sie alle Regeln hinzugefügt haben, wählen Sie Create (Erstellen) aus.

Sie können Ihre Regelgruppe testen, indem Sie sie einer AWS WAF WebACL hinzufügen und die WebACL-Aktion auf Override to Count setzen. Diese Aktion überschreibt alle Aktionen, die Sie für die in der Gruppe enthaltenen Regeln auswählen, und zählt nur übereinstimmende Anforderungen. Weitere Informationen finden Sie unter [Erstellen einer Web-ACL](#).

Hinzufügen und Löschen von Regeln aus einer AWS WAF klassischen Regelgruppe

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#).

Sie können Regeln in einer AWS WAF klassischen Regelgruppe hinzufügen oder löschen.

Wenn eine Regel aus der Regelgruppe gelöscht wird, wird die Regel selbst nicht gelöscht. Die Regel wird nur aus der Regelgruppe entfernt.

So verfahren Sie zum Hinzufügen oder Löschen von Regeln in einer Regelgruppe (Konsole)


1. Melden Sie sich AWS Management Console mit dem AWS Firewall Manager Administratorkonto an, das Sie in den Voraussetzungen eingerichtet haben, und öffnen Sie dann die Firewall Manager Konsole unter <https://console.aws.amazon.com/wafv2/fms>.

Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [Schritt 2: Erstellen Sie ein AWS Firewall Manager Standard-Administratorkonto](#).

2. Wählen Sie im Navigationsbereich die Option Zu AWS WAF Classic wechseln aus.
3. Wählen Sie im AWS WAF klassischen Navigationsbereich die Option Regelgruppen aus.
4. Wählen Sie die Regelgruppe aus, die Sie bearbeiten möchten.
5. Wählen Sie Edit rule group (Regelgruppe bearbeiten).


6. Um Regeln hinzuzufügen, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie eine Regel und anschließend Add rule to rule group (Regel zur Regelgruppe hinzufügen) aus. Wählen Sie aus, ob Anforderungen zugelassen, blockiert oder gezählt werden sollen, die mit den Bedingungen der Regel übereinstimmen. Weitere Informationen zu den Optionen finden Sie unter [So funktioniert AWS WAF Classic](#). Wiederholen Sie den Vorgang, um der Regelgruppe weitere Regeln hinzuzufügen.

 Note

Sie können keine ratenbasierten Regeln zur Regelgruppe hinzufügen.

- b. Wählen Sie Aktualisieren.
7. Um Regeln zu löschen, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie X neben der Regel, die Sie löschen möchten. Wiederholen Sie den Vorgang, um weitere Regeln aus der Regelgruppe zu löschen.
 - b. Wählen Sie Aktualisieren.

Erste Schritte mit AWS Firewall Manager , um AWS WAF klassische Regeln zu aktivieren

 Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter. [AWS WAF](#)

Sie können AWS Firewall Manager AWS WAF Regeln, AWS WAF klassische Regeln, AWS Shield Advanced Schutzmaßnahmen und Amazon VPC-Sicherheitsgruppen aktivieren. Die Schritte zum Einrichten sind dafür jeweils etwas unterschiedlich:

- Wenn Sie den Firewall Manager verwenden möchten, um Regeln mit der neuesten Version von zu aktivieren AWS WAF, verwenden Sie dieses Thema nicht. Führen Sie stattdessen die Schritte in [Erste Schritte mit AWS Firewall Manager AWS WAF Richtlinien](#) aus.
- Gehen Sie wie unter beschrieben vor, um den Firewall Manager zum Aktivieren von AWS Shield Advanced Schutzmaßnahmen zu verwenden. [Erste Schritte mit AWS Firewall Manager AWS Shield Advanced Richtlinien](#)
- Um den Firewall Manager zur Aktivierung von Amazon VPC-Sicherheitsgruppen zu verwenden, folgen Sie den Schritten unter [Erste Schritte mit AWS Firewall Manager Amazon VPC-Sicherheitsgruppenrichtlinien](#).

Um den Firewall Manager zur Aktivierung der AWS WAF klassischen Regeln zu verwenden, führen Sie die folgenden Schritte nacheinander aus.

Themen

- [Schritt 1: Erfüllen der Voraussetzungen](#)
- [Schritt 2: Erstellen von Regeln](#)
- [Schritt 3: Erstellen einer Regelgruppe](#)
- [Schritt 4: Eine AWS Firewall Manager AWS WAF Classic-Richtlinie erstellen und anwenden](#)

Schritt 1: Erfüllen der Voraussetzungen

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter. [AWS WAF](#)

Mehrere Schritte sind zur Vorbereitung Ihres Kontos auf AWS Firewall Manager zwingend erforderlich. Diese Schritte werden in [AWS Firewall Manager Voraussetzungen](#) beschrieben. Erfüllen Sie alle Voraussetzungen, bevor Sie mit [Schritt 2: Erstellen von Regeln](#) fortfahren.

Schritt 2: Erstellen von Regeln

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#).

In diesem Schritt erstellen Sie Regeln mit AWS WAF Classic. Wenn Sie bereits über AWS WAF Classic-Regeln verfügen, die Sie mit verwenden möchten AWS Firewall Manager, überspringen Sie diesen Schritt und fahren Sie mit fort [Schritt 3: Erstellen einer Regelgruppe](#).

Note

Verwenden Sie die AWS WAF Classic-Konsole, um Ihre Regeln zu erstellen.

Um AWS WAF klassische Regeln zu erstellen (Konsole)

- Erstellen Sie Ihre Regeln und fügen Sie Ihre Bedingungen zu Ihren Regeln hinzu. Weitere Informationen finden Sie unter [Erstellen einer Regel und Hinzufügen von Bedingungen](#).

Sie können nun mit [Schritt 3: Erstellen einer Regelgruppe](#) fortfahren.

Schritt 3: Erstellen einer Regelgruppe

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Eine Regelgruppe ist ein Satz von Regeln, der bestimmt, welche Aktionen ausgeführt werden soll, wenn ein bestimmter Satz von Bedingungen erfüllt wird. Sie können verwaltete Regelgruppen von AWS Marketplace verwenden und eigene Regelgruppen erstellen. Informationen zu verwalteten Regelgruppen finden Sie unter [AWS Marketplace Regelgruppen](#).

Um Ihre eigene Sicherheitsgruppe zu erstellen, führen Sie das folgende Verfahren durch.

So erstellen Sie eine Regelgruppe (Konsole)

1. Melden Sie sich AWS Management Console mit dem AWS Firewall Manager Administratorkonto an, das Sie in den Voraussetzungen eingerichtet haben, und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fms>.
2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wenn Sie die Voraussetzungen nicht erfüllen, zeigt die Konsole Anweisungen zum Beheben vorliegender Problemen an. Befolgen Sie die Anweisungen und beginnen Sie dann erneut mit diesem Schritt (Erstellen einer Regelgruppe). Wenn die Voraussetzungen erfüllt sind, klicken Sie auf Close (Schließen).
4. Wählen Sie Richtlinie erstellen aus.

Wählen Sie unter Policy type (Richtlinientyp) die Option AWS WAF Classic aus.

5. Wählen Sie AWS Firewall Manager Richtlinie erstellen und fügen Sie eine neue Regelgruppe hinzu.
6. Wählen Sie eine AWS-Region und dann Weiter.
7. Da Sie bereits Regeln erstellt haben, müssen Sie keine Bedingungen erstellen. Wählen Sie Weiter aus.
8. Da Sie bereits Regeln erstellt haben, müssen Sie keine Regeln erstellen. Wählen Sie Weiter aus.
9. Wählen Sie Create rule group (Regelgruppe erstellen).
10. Geben Sie für Name einen benutzerfreundlichen Namen ein.
11. Geben Sie einen Namen für die CloudWatch Metrik ein, die AWS WAF Classic erstellt und der Regelgruppe zuordnet. Der Name darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) oder die folgenden Sonderzeichen enthalten: _-! "# +*},./ . Es darf keine Leerzeichen enthalten.
12. Wählen Sie eine Regel und danach Add rule (Regel hinzufügen) aus. Eine Regel besitzt eine Aktionseinstellung, mit der Sie auswählen können, ob Anforderungen zugelassen, blockiert oder

gezählt werden sollen, die mit den Bedingungen der Regel übereinstimmen. Wählen Sie für dieses Tutorial Count (Zählen). Wiederholen Sie diesen Schritt, bis Sie alle gewünschten Regeln zur Regelgruppe hinzugefügt haben.

13. Wählen Sie Erstellen.

Sie können nun mit [Schritt 4: Eine AWS Firewall Manager AWS WAF Classic-Richtlinie erstellen und anwenden](#) fortfahren.

Schritt 4: Eine AWS Firewall Manager AWS WAF Classic-Richtlinie erstellen und anwenden

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#).


Nachdem Sie die Regelgruppe erstellt haben, erstellen Sie eine AWS Firewall Manager AWS WAF Richtlinie. Eine Firewall Manager AWS WAF Manager-Richtlinie enthält die Regelgruppe, die Sie auf Ihre Ressourcen anwenden möchten.

So erstellen Sie eine Firewall Manager AWS WAF Manager-Richtlinie (Konsole)

1. Nach dem Erstellen der Regelgruppe (der letzte Schritt im vorhergehenden Verfahren, [Schritt 3: Erstellen einer Regelgruppe](#)) zeigt die Konsole die Seite Rule group summary (Regelgruppen-Übersicht) an. Wählen Sie Weiter aus.
2. Geben Sie für Name einen benutzerfreundlichen Namen ein.
3. Wählen Sie unter Policy type (Richtlinientyp) die Option WAF aus.
4. Wählen Sie für Region eine AWS-Region. Um CloudFront Amazon-Ressourcen zu schützen, wählen Sie Global.

Um Ressourcen in mehreren Regionen (außer CloudFront Ressourcen) zu schützen, müssen Sie separate Firewall Manager Manager-Richtlinien für jede Region erstellen.

5. Wählen Sie eine hinzuzufügende Regelgruppe und danach Add rule group (Regelgruppe hinzufügen) aus.
6. Für eine Richtlinie sind zwei mögliche Aktionen vorhanden: Action set by rule group (Aktion durch Regelgruppe festgelegt) und Count (Zählen). Wenn Sie die Richtlinie und Regelgruppe testen möchten, legen Sie als Aktion Count (Zählen) fest. Diese Aktion setzt alle block (Blockieren)-Aktionen außer Kraft, die durch die in der Richtlinie enthaltene Regelgruppe angegeben werden. Wenn als Aktion der Richtlinie Count (Zählen) festgelegt ist, bedeutet dies, dass solche Anforderungen nur gezählt und nicht blockiert werden. Wenn Sie als Aktion der Richtlinie dagegen Action set by rule group (Aktion durch Regelgruppe festgelegt) festlegen, werden Aktionen der Regelgruppe in der Richtlinie verwendet. Wählen Sie für dieses Tutorial Count (Zählen).
7. Wählen Sie Weiter aus.
8. Wenn Sie nur bestimmte Konten in die Richtlinie aufnehmen oder alternativ bestimmte Konten von der Richtlinie ausschließen möchten, wählen Sie Select accounts to include/exclude from this policy (optional) (Konten auswählen, die in diese Richtlinie aufgenommen/von dieser Richtlinie ausgenommen werden sollen (optional)). Wählen Sie entweder Include only these accounts in this policy (Nur diese Konten in diese Richtlinie einschließen) oder Exclude these accounts from this policy (Diese Konten aus dieser Richtlinie ausschließen). Sie können nur eine Option auswählen. Wählen Sie Hinzufügen aus. Wählen Sie die ein- oder auszuschließenden Kontonummern und anschließend OK.

 Note

Wenn Sie diese Option nicht auswählen, wendet Firewall Manager eine Richtlinie auf alle Konten in Ihrer Organisation in an AWS Organizations. Wenn Sie ein neues Konto zur Organisation hinzufügen, wendet Firewall-Manager die Richtlinie automatisch auf das betreffende Konto an.

9. Wählen Sie die Ressourcentypen aus, die geschützt werden sollen.
10. Wenn Sie nur Ressourcen mit bestimmten Tags schützen oder alternativ Ressourcen mit bestimmten Tags ausschließen möchten, wählen Sie Use tags to include/exclude resources (Ressourcen mittels Tags ein-/ausschließen), geben Sie die Tags ein, und wählen Sie entweder Include (Einschließen) oder Exclude (Ausschließen). Sie können nur eine Option auswählen.

Wenn Sie mehr als einen Tag (durch Kommas getrennt) eingeben und eine Ressource über einen dieser Tags verfügt, gilt dies als Entsprechung.

Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).

11. Wählen Sie Create and apply this policy to existing and new resources (Erstellen und Anwenden dieser Richtlinie auf vorhandene und neue Ressourcen).

Diese Option erstellt eine Web-ACL für jedes entsprechende Konto innerhalb einer Organisation in AWS Organizations und ordnet die Web-ACL den angegebenen Ressourcen in den Konten zu. Diese Option wendet die Richtlinie auch auf alle neuen Ressourcen an, die den voranstehenden Kriterien (Ressourcentyp und Tags) entsprechen. Wenn Sie „Erstellen“ wählen, aber diese Richtlinie nicht auf bestehende oder neue Ressourcen anwenden, erstellt Firewall Manager alternativ eine Web-ACL für jedes entsprechende Konto innerhalb der Organisation, wendet die Web-ACL jedoch nicht auf Ressourcen an. Sie müssen die Richtlinie zu einem späteren Zeitpunkt auf Ressourcen anwenden.

12. Behalten Sie für die Option Replace existing associated web ACLs (Vorhandene zugeordnete Web-ACLs ersetzen) die Standardeinstellung bei.

Wenn diese Option ausgewählt ist, hat Firewall Manager alle vorhandenen Web-ACL-Zuordnungen aus Ressourcen im Geltungsbereich entfernt, bevor er ihnen die Web-ACLs der neuen Richtlinie zuordnet.

13. Wählen Sie Weiter aus.
14. Überprüfen Sie die neue Richtlinie. Um Änderungen vorzunehmen, wählen Sie Edit (Bearbeiten). Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen).

Tutorial: Erstellen einer AWS Firewall Manager-Richtlinie mit hierarchischen Regeln

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Mit AWS Firewall Manager können Sie AWS WAF klassische Schutzrichtlinien erstellen und anwenden, die hierarchische Regeln enthalten. Das heißt, Sie können bestimmte Regeln zentral erstellen und durchsetzen, die Erstellung und Wartung kontospezifischer Regeln aber anderen Personen überlassen. Sie können die zentral angewendeten (gemeinsamen) Regeln auf versehentliches Entfernen oder fehlerhafte Behandlung überwachen und so ihre konsistente Anwendung sicherstellen. Die kontospezifischen Regeln bieten weiteren an die Anforderungen einzelner Teams angepassten Schutz hinzu.

Note

In der neuesten Version von AWS WAF ist diese Funktion integriert und erfordert keine besondere Behandlung. Wenn Sie AWS WAF Classic noch nicht verwenden, verwenden Sie stattdessen die neueste Version. Siehe [Eine AWS Firewall Manager Richtlinie erstellen für AWS WAF](#).

Das folgende Tutorial beschreibt die Erstellung eines hierarchischen Satzes von Schutzregeln.

Themen

- [Schritt 1: Bestimmen Sie ein Firewall Manager Manager-Administratorkonto](#)
- [Schritt 2: Erstellen Sie eine Regelgruppe mit dem Firewall Manager Manager-Administratorkonto](#)
- [Schritt 3: Erstellen Sie eine Firewall Manager Manager-Richtlinie und fügen Sie die allgemeine Regelgruppe hinzu](#)
- [Schritt 4: Hinzufügen kontospezifischer Regeln](#)
- [Schlussfolgerung](#)

Schritt 1: Bestimmen Sie ein Firewall Manager Manager-Administratorkonto

Zur Verwendung AWS Firewall Manager müssen Sie ein Konto in Ihrer Organisation als Firewall Manager Manager-Administratorkonto festlegen. Dieses Konto kann entweder das Verwaltungskonto oder ein Mitgliedskonto in der Organisation sein.

Sie können das Firewall Manager Manager-Administratorkonto verwenden, um eine Reihe allgemeiner Regeln zu erstellen, die Sie auf andere Konten in der Organisation anwenden. Andere Konten in der Organisation können diese zentral angewendeten Regeln nicht ändern.

Um ein Konto als Firewall Manager-Administratorkonto festzulegen und weitere Voraussetzungen für die Verwendung von Firewall Manager zu erfüllen, finden Sie die Anweisungen unter [AWS Firewall Manager Voraussetzungen](#). Wenn die Voraussetzungen bereits erfüllt sind, können Sie zu Schritt 2 dieses Tutorials springen.

In diesem Tutorial bezeichnen wir das Administratorkonto als **Firewall-Administrator-Account**.

Schritt 2: Erstellen Sie eine Regelgruppe mit dem Firewall Manager Manager-Administratorkonto

Erstellen Sie dann mithilfe von **Firewall-Administrator-Account** eine Regelgruppe. Diese Regelgruppe enthält die gemeinsamen Regeln, die Sie für alle Mitgliedskonten anwenden, die der im nächsten Schritt erstellten Richtlinie unterliegen. Nur das **Firewall-Administrator-Account** kann Änderungen an diesen Regeln und der Container-Regelgruppe vornehmen.

In diesem Tutorial bezeichnen wir diese Container-Regelgruppe als **Common-Rule-Group**.

Zur Erstellung einer Regelgruppe vgl. die Anweisungen in [Eine AWS WAF klassische Regelgruppe erstellen](#). Denken Sie daran, sich mit Ihrem Firewall Manager Manager-Administratorkonto (**Firewall-Administrator-Account**) bei der Konsole anzumelden, wenn Sie diese Anweisungen befolgen.

Schritt 3: Erstellen Sie eine Firewall Manager Manager-Richtlinie und fügen Sie die allgemeine Regelgruppe hinzu

Erstellen Sie mit **Firewall-Administrator-Account**, eine Firewall Manager Manager-Richtlinie. Wenn Sie diese Richtlinie erstellen, müssen Sie Folgendes tun:

- Fügen Sie **Common-Rule-Group** zu der neuen Richtlinie hinzu.
- Schließen Sie alle Konten in der Organisation ein, auf die **Common-Rule-Group** angewendet werden soll.
- Fügen Sie alle Ressourcen hinzu, auf die **Common-Rule-Group** angewendet werden soll.

Anleitungen zum Erstellen einer Richtlinie finden Sie unter [Eine AWS Firewall Manager Richtlinie erstellen](#).

Dadurch wird eine Web-ACL in jedem angegebenen Konto erstellt und **Common-Rule-Group** jeder dieser Web-ACLs hinzugefügt. Nachdem Sie die Richtlinie erstellt haben, werden diese Web-ACL und die gemeinsamen Regeln für alle angegebenen Konten bereitgestellt.

In diesem Tutorial bezeichnen wir diese Web-ACL als **Administrator-Created-ACL**. Jetzt besteht in jedem angegebenen Mitgliedskonto der Organisation eine eindeutige **Administrator-Created-ACL**.

Schritt 4: Hinzufügen kontospezifischer Regeln

Jedes Mitgliedskonto der Organisation kann jetzt seine eigenen kontospezifischen Regeln zu der **Administrator-Created-ACL** in ihrem Konto hinzufügen. Die bereits geltenden allgemeinen Regeln gelten **Administrator-Created-ACL** weiterhin, ebenso wie die neuen, kontospezifischen Regeln. AWS WAF prüft Webanfragen anhand der Reihenfolge, in der die Regeln in der Web-ACL erscheinen. Dies gilt für **Administrator-Created-ACL** und für kontospezifische Regeln.

Informationen zum Hinzufügen von Regeln finden Sie **Administrator-Created-ACL** unter [Bearbeiten einer Web-ACL](#).

Schlussfolgerung

Sie verfügen jetzt über eine Web-ACL, die allgemeine Regeln enthält, die vom Firewall Manager Administratorkonto verwaltet werden, sowie kontospezifische Regeln, die von jedem Mitgliedskonto verwaltet werden.

Die **Administrator-Created-ACL** in jedem Konto verweist auf die einzelnen Referenzen **Common-Rule-Group**. Daher werden future Änderungen durch das Firewall Manager Administratorkonto **Common-Rule-Group** sofort für jedes Mitgliedskonto wirksam.

Mitgliedskonten können die gemeinsamen Regeln in **Common-Rule-Group** nicht ändern oder entfernen.

Kontospezifische Regeln wirken sich nicht auf andere Konten aus.

Protokollieren von Web-ACL-Traffic-Informationen

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November

2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Sie können die Protokollierung aktivieren, um detaillierte Informationen über den Traffic zu erhalten, der von Ihrer Web-ACL analysiert wird. Zu den Informationen, die in den Protokollen enthalten sind, gehören der Zeitpunkt, zu dem AWS WAF Classic die Anfrage von Ihrer AWS Ressource erhalten hat, detaillierte Informationen zu der Anfrage und die Aktion für die Regel, der jede Anfrage entsprach.

Um zu beginnen, richten Sie einen Amazon Kinesis Data Firehose ein. Wählen Sie im Rahmen dieses Prozesses ein Ziel zur Speicherung Ihrer Protokolle aus. Als Nächstes wählen Sie die Web-ACL aus, für die Sie die Protokollierung aktivieren möchten. Nachdem Sie die Protokollierung aktiviert haben AWS WAF, werden die Protokolle über die Firehose an Ihr Speicherziel gesendet.

Informationen zum Erstellen einer Amazon Kinesis Data Firehose und zum Überprüfen Ihrer gespeicherten Protokolle finden Sie unter [Was ist Amazon Data Firehose?](#) Informationen zu den für Ihre Kinesis-Data-Firehose-Konfiguration erforderlichen Berechtigungen finden Sie unter [Controlling Access with Amazon Kinesis Data Firehose](#) (Zugriff mit Amazon Kinesis Data Firehose steuern).

Sie müssen über die folgenden Berechtigungen verfügen, um erfolgreich die Protokollierung zu aktivieren:

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `waf:PutLoggingConfiguration`

Weitere Informationen zu serviceverknüpften Rollen und zur Berechtigung

`iam:CreateServiceLinkedRole` finden Sie unter [Verwenden von serviceverknüpften Rollen für Classic AWS WAF](#).

Aktivieren der Protokollierung für eine Web-ACL

1. Erstellen Sie eine Amazon Kinesis Data Firehose mit einem Namen, der mit dem Präfix "aws-waf-logs-" beginnt. Beispiel: `aws-waf-logs-us-east-2-analytics` Erstellen Sie den Data Firehose mit einer PUT-Quelle und in der Region, in der Sie aktiv sind. Wenn Sie Logs für

Amazon erfassen CloudFront, erstellen Sie die Firehose in USA East (Nord-Virginia). Weitere Informationen finden Sie unter [Amazon Data Firehose Delivery Stream erstellen](#).

 **Important**


Wählen Sie nicht Kinesis stream als Ihre Quelle.

Ein AWS WAF Classic-Protokoll entspricht einem Firehose-Datensatz. Wenn Sie normalerweise 10.000 Anfragen pro Sekunde erhalten und vollständige Protokolle aktivieren, sollten Sie in Firehose eine Einstellung von 10.000 Datensätzen pro Sekunde haben. Wenn Sie Firehose nicht richtig konfigurieren, zeichnet AWS WAF Classic nicht alle Protokolle auf. Weitere Informationen finden Sie unter [Amazon Kinesis Data Firehose-Kontingente](#).

2. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter <https://console.aws.amazon.com/wafv2/>.

Wenn im Navigationsbereich zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

3. Wählen Sie im Navigationsbereich Web ACLs aus.
4. Wählen Sie die Web-ACL aus, für die Sie die Protokollierung aktivieren möchten. Dadurch wird im rechten Bereich eine Seite mit den Details der Web-ACL geöffnet.
5. Klicken Sie auf der Registerkarte Logging (Protokollieren) auf Enable logging (Protokollieren aktivieren).
6. Wählen Sie den Kinesis Data Firehose, den Sie im ersten Schritt erstellt haben. Sie müssen einen Firehose wählen, der mit "aws-waf-logs-" beginnt.
7. (Optional) Wenn Sie nicht möchten, dass bestimmte Felder und deren Werte in den Protokollen enthalten sind, machen Sie diese Felder unkenntlich. Wählen Sie das Feld aus, das unkenntlich gemacht werden soll, und klicken Sie dann auf Add (Hinzufügen). Wiederholen Sie diesen Vorgang nach Bedarf, um zusätzliche Felder unkenntlich zu machen. Die unkenntlich gemachten Felder werden als REDACTED in den Protokollen angezeigt. Wenn Sie beispielsweise das Feld Cookie unkenntlich machen, wird das Feld Cookie in den Protokollen als REDACTED angezeigt.
8. Wählen Sie Enable logging (Protokollierung aktivieren) aus.

 **Note**

Wenn Sie die Protokollierung erfolgreich aktivieren, erstellt AWS WAF Classic eine serviceverknüpfte Rolle mit den erforderlichen Berechtigungen, um Protokolle in die

Amazon Kinesis Data Firehose zu schreiben. Weitere Informationen finden Sie unter [Verwenden von serviceverknüpften Rollen für Classic AWS WAF](#).

Deaktivieren der Protokollierung für eine Web-ACL

1. Wählen Sie im Navigationsbereich Web ACLs aus.
2. Wählen Sie die Web-ACL aus, für die Sie die Protokollierung deaktivieren möchten. Dadurch wird im rechten Bereich eine Seite mit den Details der Web-ACL geöffnet.
3. Klicken Sie auf der Registerkarte Logging (Protokollieren) auf Disable logging (Protokollieren deaktivieren).
4. Wählen Sie im Dialogfeld Disable logging (Protokollieren deaktivieren).

Example Beispielprotokoll

```
{
  "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": "username=abc",
      "httpVersion": "HTTP/1.1",
      "httpMethod": "GET",
      "requestId": "cloud front Request id"
    }
  }
```

Im Folgenden finden Sie Beschreibungen aller Elemente, die in diesen Protokollen aufgelistet werden.

Zeitstempel

Der Zeitstempel in Millisekunden.

formatVersion

Die Formatversion für das Protokoll.

webaclId

Die GUID der Web-ACL.

terminatingRuleId

Die ID der Regel, die die Anforderung beendet. Wenn nichts zur Beendigung der Anforderung führt, ist der Wert `Default_Action`.

terminatingRuleType

Der Typ der Regel, die die Anforderung beendet. Mögliche Werte: `RATE_BASED`, `REGULAR` und `GROUP`.

action

Die Aktion. Mögliche Werte für eine beendende Regel: `ALLOW` und `BLOCK`. `COUNT` ist kein gültiger Wert für eine beendende Regel.

terminatingRuleMatchEinzelheiten

Detaillierte Informationen zur Beendigungsregel, die mit der Anforderung übereingestimmt hat. Eine Beendigungsregel verfügt über eine Aktion, die den Inspektionsprozess für eine Webanforderung beendet. Mögliche Aktionen für Beendigungsregeln sind

ALLOW und BLOCK. Dies wird nur für SQL-Injection und Cross-Site Scripting (XSS) - Übereinstimmungsregelanweisungen aufgefüllt. Wie bei allen Regelanweisungen, die auf mehr als ein Element prüfen, wendet AWS WAF die Aktion auf die erste Übereinstimmung an und stoppt die Überprüfung der Webanforderung. Eine Webanforderung mit einer Beendungsaktion kann zusätzlich zu den im Protokoll gemeldeten Bedrohungen weitere Bedrohungen enthalten.

httpSourceName

Die Quelle der Anforderung. Mögliche Werte: CF (wenn die Quelle Amazon ist CloudFront), APIGW (wenn die Quelle Amazon API Gateway ist) und ALB (wenn die Quelle ein Application Load Balancer ist).

httpSourceId

Die Quell-ID. Dieses Feld zeigt die ID der zugehörigen CloudFront Amazon-Distribution, die REST-API für API Gateway oder den Namen für einen Application Load Balancer.

ruleGroupList

Die Liste der Regelgruppen, die auf diese Anforderung reagiert haben. Im vorangehenden Beispiel gibt es nur eine.

ruleGroupId

Die ID der Regelgruppe. Wenn die Regel die Anforderung blockiert hat, ist die ID für `ruleGroupId` mit der ID für `terminatingRuleId` identisch.

terminatingRule

Die Regel innerhalb der Regelgruppe, die die Anforderung beendet hat. Wenn es sich um einen Nicht-Null-Wert handelt, enthält er auch eine `ruleId` (Regel-ID) und eine `action` (Aktion). In diesem Fall ist die Aktion stets BLOCK.

nonTerminatingMatchingRegeln

Die Liste der Regeln in der Regelgruppe, die mit der Anforderung übereinstimmen. Dies sind stets COUNT-Regeln (nicht beendende Regeln, die übereinstimmen).

Aktion (Gruppe nonTerminatingMatching Regeln)

Dies ist stets COUNT (nicht beendende Regeln, die übereinstimmen).

ruleId (nonTerminatingMatchingRegelgruppe)

Die ID der Regel innerhalb der Regelgruppe, die mit der Anforderung übereinstimmt und nicht beendend war. Also COUNT-Regeln.

excludedRules

Die Liste der Regeln in der Regelgruppe, die von Ihnen ausgeschlossen wurden. Die Aktion für diese Regeln ist auf COUNT festgelegt.

exclusionType (excludedRules-Gruppe)

Ein Typ, der anzeigt, dass die ausgeschlossene Regel die Aktion COUNT hat.

ruleId (excludedRules-Gruppe)

Die ID der Regel innerhalb der Regelgruppe, die ausgeschlossen ist.

rateBasedRuleListe

Die Liste der ratenbasierten Regeln, die auf die Anforderung reagiert haben.

rateBasedRuleID

Die ID der ratenbasierten Regel, die auf die Anforderung reagiert hat. Wenn die Anforderung hierdurch beendet wurde, ist die ID für `rateBasedRuleId` mit der ID für `terminatingRuleId` identisch.

limitKey

Das Feld, AWS WAF anhand dessen bestimmt wird, ob Anfragen wahrscheinlich aus einer einzigen Quelle stammen und daher einer Tarifüberwachung unterliegen. Möglicher Wert: IP.

maxRateAllowed

Die maximale Anzahl von Anforderungen mit einem identischen Wert in dem Feld, das durch `limitKey` angegeben wird, zulässig innerhalb eines Zeitraums von fünf Minuten. Wenn die Anzahl der Anfragen den Wert überschreitet `maxRateAllowed` und die anderen in der Regel angegebenen Prädikate ebenfalls erfüllt sind, wird die für diese Regel angegebene Aktion AWS WAF ausgelöst.

httpRequest

Die Metadaten zu der Anforderung.

clientIp

Die IP-Adresse des Clients, der die Anforderung sendet.

country

Das Quellland der Anforderung. Wenn AWS WAF das Herkunftsland nicht bestimmt werden kann, wird dieses Feld auf gesetzt. -

Header

Die Liste der Header.

uri

Der URI der Anforderung. Das vorangehende Codebeispiel zeigt, wie der Wert aussehen würde, wenn dieses Feld redigiert worden wäre.

args

Die Abfragezeichenfolge.

httpVersion

Die HTTP-Version.

httpMethod

Die HTTP-Methode in der Anforderung.

requestId

Die ID der Anfrage.

Auflisten der durch ratenbasierte Regeln blockierten IP-Adressen

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#).

AWS WAF Classic bietet eine Liste von IP-Adressen, die durch ratenbasierte Regeln blockiert werden.

So listen Sie die durch ratenbasierte Regeln blockierten IP-Adressen auf

1. [Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS WAF Konsole unter https://console.aws.amazon.com/wafv2/.](https://console.aws.amazon.com/wafv2/)

Wenn im Navigationsbereich die Option Zu AWS WAF Classic wechseln angezeigt wird, wählen Sie es aus.

2. Wählen Sie im Navigationsbereich Regeln aus.
3. Wählen Sie in der Spalte Name eine ratenbasierte Regel aus.

Die Liste zeigt die IP-Adressen an, die die Regel derzeit blockiert.

So funktioniert AWS WAF Classic mit CloudFront Amazon-Funktionen

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Wenn Sie eine Web-ACL erstellen, können Sie eine oder mehrere CloudFront Distributionen angeben, die AWS WAF Classic untersuchen soll. AWS WAF Classic beginnt, Webanfragen für diese Distributionen auf der Grundlage der Bedingungen, die Sie in der Web-ACL angeben, zuzulassen, zu blockieren oder zu zählen. CloudFront bietet einige Funktionen, die die AWS WAF Classic-Funktionalität erweitern. In diesem Kapitel werden einige Möglichkeiten beschrieben, die Sie konfigurieren können CloudFront , damit AWS WAF Classic CloudFront und Classic besser zusammenarbeiten.

Themen

- [Verwenden von AWS WAF Classic mit CloudFront benutzerdefinierten Fehlerseiten](#)
- [Verwenden Sie AWS WAF Classic mit CloudFront für Anwendungen, die auf Ihrem eigenen HTTP-Server ausgeführt werden](#)
- [Auswahl der HTTP-Methoden, die CloudFront darauf reagieren](#)

Verwenden von AWS WAF Classic mit CloudFront benutzerdefinierten Fehlerseiten

Wenn AWS WAF Classic eine Webanforderung auf der Grundlage der von Ihnen angegebenen Bedingungen blockiert, wird der HTTP-Statuscode 403 (Forbidden) an zurückgegeben CloudFront. Als Nächstes wird dieser Statuscode an den Betrachter CloudFront zurückgegeben. Dieses zeigt dann die folgende kurze und kaum formatierte Standardnachricht an:

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

Wenn Sie lieber eine benutzerdefinierte Fehlermeldung anzeigen möchten, die möglicherweise dieselbe Formatierung wie der Rest Ihrer Website verwendet, können Sie so konfigurieren CloudFront , dass ein Objekt (z. B. eine HTML-Datei), das Ihre benutzerdefinierte Fehlermeldung enthält, an den Viewer zurückgegeben wird.

Note

CloudFront kann nicht zwischen einem HTTP-Statuscode 403, der von Ihrem Ursprung zurückgegeben wird, und einem, der von AWS WAF Classic zurückgegeben wird, wenn eine Anfrage blockiert wird, unterscheiden. Das heißt, Sie können keine unterschiedlichen benutzerdefinierten Fehlerseiten basierend auf den verschiedenen Ursachen für den HTTP-Statuscode 403 zurückgeben.

Weitere Informationen zu CloudFront benutzerdefinierten Fehlerseiten finden Sie unter [Anpassen von Fehlerantworten](#) im Amazon CloudFront Developer Guide.

Verwenden Sie AWS WAF Classic mit CloudFront für Anwendungen, die auf Ihrem eigenen HTTP-Server ausgeführt werden

Wenn Sie AWS WAF Classic mit verwenden CloudFront, können Sie Ihre Anwendungen schützen, die auf einem beliebigen HTTP-Webserver ausgeführt werden, unabhängig davon, ob es sich um einen Webserver handelt, der in Amazon Elastic Compute Cloud (Amazon EC2) läuft, oder um einen Webserver, den Sie privat verwalten. Sie können auch so konfigurieren CloudFront , dass HTTPS zwischen CloudFront und Ihrem eigenen Webserver sowie zwischen Zuschauern und erforderlich ist. CloudFront

HTTPS zwischen CloudFront und Ihrem eigenen Webserver ist erforderlich

Um HTTPS zwischen CloudFront und Ihrem eigenen Webserver zu verlangen, können Sie die CloudFront benutzerdefinierte Origin-Funktion verwenden und die Origin-Protokollrichtlinie und die Einstellungen für den Origin-Domainnamen für bestimmte Ursprünge konfigurieren. In Ihrer CloudFront Konfiguration können Sie den DNS-Namen des Servers zusammen mit dem Port und dem Protokoll angeben, das Sie beim Abrufen von Objekten von Ihrem Ursprung verwenden CloudFront möchten. Außerdem sollten Sie sicherstellen, dass das SSL/TLS-Zertifikat auf Ihrem benutzerdefinierten Ursprungs-Server mit dem von Ihnen konfigurierten Ursprungsdomänennamen übereinstimmt. Wenn Sie Ihren eigenen HTTP-Webserver außerhalb von verwenden AWS, müssen Sie ein Zertifikat verwenden, das von einer vertrauenswürdigen Zertifizierungsstelle (CA) eines Drittanbieters, z. B. Comodo oder Symantec, signiert wurde. DigiCert Weitere Informationen darüber, wie HTTPS für die Kommunikation zwischen Ihrem eigenen Webserver CloudFront und Ihrem eigenen Webserver [erforderlich ist, finden Sie im Amazon CloudFront Developer Guide unter HTTPS für die Kommunikation zwischen CloudFront und Ihrem benutzerdefinierten Ursprung](#) erforderlich.

HTTPS zwischen einem Betrachter und CloudFront

Um HTTPS zwischen Zuschauern und vorzuschreiben CloudFront, können Sie die Viewer-Protokollrichtlinie für ein oder mehrere Cache-Verhaltensweisen in Ihrer CloudFront Distribution ändern. Weitere Informationen zur Verwendung von HTTPS zwischen Zuschauern und CloudFront finden Sie im Thema [HTTPS für die Kommunikation zwischen Zuschauern erforderlich und CloudFront](#) im Amazon CloudFront Developer Guide. Sie können auch Ihr eigenes SSL-Zertifikat mitbringen, damit Zuschauer über HTTPS eine Verbindung zu Ihrer CloudFront Distribution herstellen können, indem Sie Ihren eigenen Domainnamen verwenden, zum Beispiel `https://www.mysite.com`. Weitere Informationen finden Sie im Thema [Konfiguration alternativer Domainnamen und HTTPS](#) im Amazon CloudFront Developer Guide.

Auswahl der HTTP-Methoden, die CloudFront darauf reagieren

Wenn Sie eine CloudFront Amazon-Webdistribution erstellen, wählen Sie die HTTP-Methoden aus, die Sie verarbeiten und CloudFront an Ihren Ursprung weiterleiten möchten. Sie können aus den folgenden Optionen auswählen:

- GET, HEAD — Sie können diese CloudFront Option nur verwenden, um Objekte von Ihrem Ursprung oder Objekt-Header abzurufen.
- GET, HEAD, OPTIONS — Sie können diese Option CloudFront nur verwenden, um Objekte von Ihrem Ursprung abzurufen, Objekt-Header abzurufen oder eine Liste der Optionen abzurufen, die Ihr Original-Server unterstützt.

- GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE — Sie können CloudFront sie verwenden, um Objekte abzurufen, hinzuzufügen, zu aktualisieren und zu löschen und Objekt-Header abzurufen. Darüber hinaus können Sie andere POST-Vorgänge wie das Senden von Daten aus einem Webformular ausführen.

Sie können auch AWS WAF klassische Bedingungen für den Abgleich von Zeichenketten verwenden, um Anfragen, die auf der HTTP-Methode basieren, zuzulassen oder zu blockieren, wie unter beschrieben [Arbeiten mit Zeichenfolgen-Übereinstimmungsbedingungen](#). Wenn Sie eine Kombination von Methoden verwenden möchten, die CloudFront Unterstützung bieten, z. B. GET und HEAD, müssen Sie AWS WAF Classic nicht so konfigurieren, dass Anfragen blockiert werden, die die anderen Methoden verwenden. Wenn Sie eine Kombination von Methoden zulassen möchten, die CloudFront nicht unterstützt werden, z. B., und GETHEAD, können Sie so konfigurieren POST, dass CloudFront auf alle Methoden reagiert wird, und dann AWS WAF Classic verwenden, um Anfragen zu blockieren, die andere Methoden verwenden.

Weitere Informationen zur Auswahl der Methoden, CloudFront auf die reagiert, finden Sie unter [Zulässige HTTP-Methoden](#) im Thema [Werte, die Sie beim Erstellen oder Aktualisieren einer Web-Distribution angeben](#) im Amazon CloudFront Developer Guide.

Sicherheit in AWS WAF Classic

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter. [AWS WAF](#)

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- **Sicherheit der Cloud** — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Die Wirksamkeit unserer Sicherheitsfunktionen wird regelmäßig von externen Prüfern im Rahmen des [AWS -Compliance-Programms getestet und überprüft](#). Weitere Informationen zu den Compliance-Programmen, die für AWS WAF Classic gelten, finden Sie unter [AWS Services in Scope by Compliance Program](#).
- **Sicherheit in der Cloud** — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. In Ihre Verantwortung fallen außerdem weitere Faktoren, wie z. B. die Vertraulichkeit der Daten, die Anforderungen Ihrer Organisation sowie geltende Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von AWS WAF Classic anwenden können. In den folgenden Themen erfahren Sie, wie Sie AWS WAF Classic konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste verwenden können, die Sie bei der Überwachung und Sicherung Ihrer AWS WAF Classic-Ressourcen unterstützen.

Themen

- [Datenschutz in AWS WAF Classic](#)
- [Identitäts- und Zugriffsmanagement für AWS WAF Classic](#)
- [Protokollierung und Überwachung in AWS WAF Classic](#)
- [Konformitätsvalidierung für AWS WAF Classic](#)
- [Resilienz in AWS WAF Classic](#)
- [Infrastruktursicherheit in AWS WAF Classic](#)

Datenschutz in AWS WAF Classic

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Das [Modell der AWS gemeinsamen Verantwortung](#) und geteilter Verantwortung gilt für den Datenschutz in AWS WAF Classic. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der die gesamte Infrastruktur läuft AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter [Häufig gestellte Fragen zum Datenschutz](#). Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag [AWS -Modell der geteilten Verantwortung und in der DSGVO](#) im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-2](#).

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit AWS WAF Classic oder anderen Geräten arbeiten und die Konsole, die API oder SDKs AWS-Services verwenden. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

AWS WAF Klassische Entitäten — wie Web-ACLs, Regeln und Bedingungen — werden im Ruhezustand verschlüsselt, außer in bestimmten Regionen, in denen Verschlüsselung nicht verfügbar ist, darunter China (Peking) und China (Ningxia). Eindeutige Verschlüsselungsschlüssel werden für jede Region verwendet.

AWS WAF Klassische Ressourcen werden gelöscht

Sie können die Ressourcen löschen, die Sie in AWS WAF Classic erstellt haben. In den folgenden Abschnitten finden Sie Anleitungen für die verschiedenen Ressourcentypen.

- [Löschen einer Web-ACL](#)
- [Hinzufügen und Löschen von Regeln aus einer AWS WAF klassischen Regelgruppe](#)
- [Löschen einer Regel](#)

Identitäts- und Zugriffsmanagement für AWS WAF Classic

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#).

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service, den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Classic-Ressourcen zu verwenden AWS WAF. IAM ist ein Programm AWS-Service, das Sie ohne zusätzliche Kosten nutzen können.

Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)

- [So funktioniert AWS WAF Classic mit IAM](#)
- [Beispiele für identitätsbasierte Richtlinien für Classic AWS WAF](#)
- [Problembehebung bei AWS WAF klassischer Identität und Zugriff](#)
- [Verwenden von serviceverknüpften Rollen für Classic AWS WAF](#)

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in AWS WAF Classic ausführen.

Dienstbenutzer — Wenn Sie den AWS WAF Classic-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Wenn Sie für Ihre Arbeit mehr AWS WAF Classic-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie in AWS WAF Classic nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unter [Problembehebung bei AWS WAF klassischer Identität und Zugriff](#).

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für AWS WAF Classic-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf AWS WAF Classic. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS WAF Classic-Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit AWS WAF Classic verwenden kann, finden Sie unter [So funktioniert AWS WAF Classic mit IAM](#).

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Classic schreiben können. AWS WAF Beispiele für identitätsbasierte AWS WAF Classic-Richtlinien, die Sie in IAM verwenden können, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Classic AWS WAF](#)

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportale anmelden. Weitere Informationen zur Anmeldung finden Sie [AWS unter So melden Sie sich bei Ihrem an AWS-Konto](#) im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu [signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen](#) signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter [Multi-Faktor-Authentifizierung](#) im AWS IAM Identity Center - Benutzerhandbuch und [Verwenden der Multi-Faktor-Authentifizierung \(MFA\) in AWS](#) im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie ein AWS-Konto erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter [Was ist IAM Identity Center?](#) im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Eine [IAM-Gruppe](#) ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen

bereit. Weitere Informationen finden Sie unter [Erstellen eines IAM-Benutzers \(anstatt einer Rolle\)](#) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen [wechseln](#). Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter [Verwenden von IAM-Rollen](#) im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- **Verbundbenutzerzugriff:** Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter [Erstellen von Rollen für externe Identitätsanbieter](#) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze](#) im AWS IAM Identity Center -Benutzerhandbuch.
- **Temporäre IAM-Benutzerberechtigungen:** Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- **Kontoübergreifender Zugriff –** Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien](#) im IAM-Benutzerhandbuch.
- **Serviceübergreifender Zugriff —** Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann

dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.

- **Forward Access Sessions (FAS)** — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).
- **Servicerolle:** Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.
- **Dienstbezogene Rolle** — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- **Anwendungen, die auf Amazon EC2 ausgeführt werden** — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter [Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden](#) im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter [Erstellen einer IAM-Rolle \(anstatt eines Benutzers\)](#) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie

wählen, finden Sie unter [Auswahl zwischen verwalteten und eingebundenen Richtlinien](#) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen zu ACLs finden Sie unter [Zugriffssteuerungsliste \(ACL\) – Übersicht](#) (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- **Berechtigungsgrenzen:** Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien

setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im IAM-Benutzerhandbuch.

- **Service Control Policies (SCPs)** — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten, die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organisationen und SCPs finden Sie unter [Funktionsweise von SCPs](#) im AWS Organizations -Benutzerhandbuch.
- **Sitzungsrichtlinien:** Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

So funktioniert AWS WAF Classic mit IAM

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Bevor Sie IAM zur Verwaltung des Zugriffs auf AWS WAF Classic verwenden, sollten Sie sich darüber informieren, welche IAM-Funktionen für Classic verfügbar sind. AWS WAF

IAM-Funktionen, die Sie mit Classic verwenden können AWS WAF

IAM-Feature	AWS WAF Klassische Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (servicespezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie AWS WAF Classic und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im [IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren](#).

Identitätsbasierte Richtlinien für Classic AWS WAF

Unterstützt Richtlinien auf Identitätsbasis.	Ja
--	----

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien in AWS WAF Classic finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Classic AWS WAF](#)

Ressourcenbasierte Richtlinien innerhalb von Classic AWS WAF

Unterstützt ressourcenbasierte Richtlinien	Nein
--	------

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalidentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen

finden Sie unter [Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden](#) im IAM-Benutzerhandbuch.

Richtlinienaktionen für Classic AWS WAF

Unterstützt Richtlinienaktionen

Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der AWS WAF klassischen Aktionen finden Sie in der Serviceautorisierungsreferenz unter [Aktionen definiert von AWS WAF und Aktionen, die von AWS WAF Regional](#) definiert sind.

Bei Richtlinienaktionen in AWS WAF Classic wird vor der Aktion das folgende Präfix verwendet:

```
waf
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [  
  "waf:action1",  
  "waf:action2"  
]
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Um beispielsweise alle Aktionen in AWS WAF Classic anzugeben, die mit `beginnenList` beginnen, schließen Sie die folgende Aktion ein:

```
"Action": "waf:List*"
```

Beispiele für AWS WAF klassische identitätsbasierte Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Classic AWS WAF](#)

Richtlinienressourcen für Classic AWS WAF

Unterstützt Richtlinienressourcen	Ja
-----------------------------------	----

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein `Resource` oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen [Amazon-Ressourcennamen \(ARN\)](#) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der AWS WAF klassischen Ressourcentypen und ihrer ARNs finden Sie in der Service Authorization Reference unter [Resources defined by AWS WAF](#) und [Resources defined by AWS WAF Regional](#). Informationen zu den Aktionen, mit denen Sie den ARN jeder Ressource angeben können, finden Sie unter [Aktionen definiert von AWS WAF](#) und [Aktionen definiert von AWS WAF Regional](#). Um den Zugriff auf eine Teilmenge der AWS WAF Classic-Ressourcen zuzulassen oder zu verweigern, nehmen Sie den ARN der Ressource in das `resource` Element Ihrer Richtlinie auf.

In AWS WAF Classic handelt es sich bei den Ressourcen um Web-ACLs und Regeln. AWS WAF Classic unterstützt auch Bedingungen wie Byteübereinstimmung, IP-Übereinstimmung und Größenbeschränkung.

Diesen Ressourcen und Bedingungen sind eindeutigen Amazon-Ressourcennamen (ARN) zugeordnet, wie in der folgenden Tabelle gezeigt.

Name in der AWS WAF Konsole	Name im AWS WAF SDK/CLI	ARN-Format
Web-ACL	WebACL	<code>arn:aws:waf:: <i>account</i>:webacl/<i>ID</i></code>
Regel	Rule	<code>arn:aws:waf:: <i>account</i>:rule/<i>ID</i></code>
Zeichenfolgen-Übereinstimmungsbedingung	ByteMatch Set	<code>arn:aws:waf:: <i>account</i>:bytematchset /<i>ID</i></code>
SQL Injection-s-Übereinstimmungsbedingung	SqlInjectionMatchSet	<code>arn:aws:waf:: <i>account</i>:sqlinjectionset /<i>ID</i></code>
Größenbeschränkungsbedingung	SizeConstraintSet	<code>arn:aws:waf:: <i>account</i>:sizeconstraintset /<i>ID</i></code>
IP-Übereinstimmungsbedingung	IPSet	<code>arn:aws:waf:: <i>account</i>:ipset/<i>ID</i></code>
Cross-Site-Scripting-Übereinstimmungsbedingung	XssMatchSet	<code>arn:aws:waf:: <i>account</i>:xssmatchset /<i>ID</i></code>

Um den Zugriff auf eine Teilmenge der AWS WAF Classic-Ressourcen zuzulassen oder zu verweigern, nehmen Sie den ARN der Ressource in das `resource` Element Ihrer Richtlinie auf. Die ARNs für AWS WAF Classic haben das folgende Format:

```
arn:aws:waf::account:resource/ID
```

Ersetzen Sie Variablen für *Konto*, *Ressource* und *ID* durch gültige Werte. Gültige Werte können beispielsweise folgende sein:

- *Konto*: Die ID Ihres AWS-Konto. Sie müssen einen Wert angeben.
- *Ressource*: Der Typ der AWS WAF klassischen Ressource.
- *ID*: Die ID der AWS WAF Classic-Ressource oder ein Platzhalter (*), um alle Ressourcen des angegebenen Typs anzugeben, die der angegebenen AWS-Konto Ressource zugeordnet sind.

Der folgende ARN gibt zum Beispiel alle Web-ACLs für das Konto 111122223333 an:

```
arn:aws:waf::111122223333:webacl/*
```

Bedingungsschlüssel für Richtlinien für Classic AWS WAF

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Ja
---	----

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition block`) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die [Bedingungsoperatoren](#) verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen OR Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter [IAM-Richtlinienelemente: Variablen und Tags](#) im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [Kontextschlüssel für AWS globale Bedingungen](#) im IAM-Benutzerhandbuch.

Eine Liste der AWS WAF klassischen Bedingungsschlüssel finden Sie unter [Bedingungsschlüssel für AWS WAF](#) und [von AWS WAF Regional definierte Ressourcen](#) in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter [Aktionen definiert von AWS WAF](#) und [Aktionen, die von AWS WAF Regional definiert](#) sind.

Beispiele für AWS WAF klassische identitätsbasierte Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Classic AWS WAF](#)

ACLs in Classic AWS WAF

Unterstützt ACLs

Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit Classic AWS WAF

Unterstützt ABAC (Tags in Richtlinien)

Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement einer [Richtlinie Tag-Informationen](#) an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter [Was ist ABAC?](#) im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe [Attributbasierte Zugriffskontrolle \(ABAC\)](#) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit Classic AWS WAF

Unterstützt temporäre Anmeldeinformationen	Ja
--	----

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services [funktionieren AWS-Services](#), [finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM](#).

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter [Wechseln zu einer Rolle \(Konsole\)](#) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter [Temporäre Sicherheitsanmeldeinformationen in IAM](#).

Zugriffssitzungen für AWS WAF Classic weiterleiten

Unterstützt Forward Access Sessions (FAS)	Ja
---	----

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion

in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

Servicerollen für Classic AWS WAF

Unterstützt Servicerollen	Ja
---------------------------	----

Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.

Warning

Durch das Ändern der Berechtigungen für eine Servicerolle kann die AWS WAF Classic-Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, wenn AWS WAF Classic eine Anleitung dazu bietet.

Dienstbezogene Rollen für Classic AWS WAF

Unterstützt serviceverknüpfte Rollen	Ja
--------------------------------------	----

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von AWS WAF klassischen dienstbezogenen Rollen finden Sie unter. [Verwenden von serviceverknüpften Rollen für Classic AWS WAF](#)

Beispiele für identitätsbasierte Richtlinien für Classic AWS WAF

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

Standardmäßig sind Benutzer und Rollen nicht berechtigt, AWS WAF Classic-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Einzelheiten zu den von AWS WAF Classic definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS WAF](#) und [Aktionen, Ressourcen und Bedingungsschlüssel für AWS WAF Regional](#) in der Service Authorization Reference.

Themen

- [Bewährte Methoden für Richtlinien](#)
- [Verwenden der Classic-Konsole AWS WAF](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS WAF Classic-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen

AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter [AWS -verwaltete Richtlinien](#) oder [AWS -verwaltete Richtlinien für Auftrags-Funktionen](#) im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten: Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter [Richtlinien und Berechtigungen in IAM](#) im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs: Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: Bedingung](#) im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten: IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter [Richtlinienvvalidierung zum IAM Access Analyzer](#) im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren

Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter [Konfigurieren eines MFA-geschützten API-Zugriffs](#) im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Bewährte Methoden für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

Verwenden der Classic-Konsole AWS WAF

Um auf die AWS WAF Classic-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS WAF Classic-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Benutzer, die auf die AWS Konsole zugreifen und sie verwenden können, können auch auf die AWS WAF Classic-Konsole zugreifen. Es sind keine zusätzlichen Berechtigungen erforderlich.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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": "*"
  }
]
```

Problembehebung bei AWS WAF klassischer Identität und Zugriff

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter. [AWS WAF](#)

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS WAF Classic und IAM auftreten können.

Themen

- [Ich bin nicht berechtigt, eine Aktion in AWS WAF Classic durchzuführen](#)

- [Ich bin nicht berechtigt, iam auszuführen: PassRole](#)
- [Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS WAF Classic-Ressourcen ermöglichen](#)

Ich bin nicht berechtigt, eine Aktion in AWS WAF Classic durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven `my-example-widget`-Ressource anzuzeigen, jedoch nicht über `waf:GetWidget`-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
waf:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `waf:GetWidget`-Aktion auf die `my-example-widget`-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht autorisiert sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an AWS WAF Classic übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS WAF Classic auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```


In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS WAF Classic-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffssteuerungslisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob AWS WAF Classic diese Funktionen unterstützt, finden Sie unter [So funktioniert AWS WAF Classic mit IAM](#).
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter [Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto, den Sie besitzen](#).
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter [Gewähren von Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien](#) im IAM-Benutzerhandbuch.

Verwenden von serviceverknüpften Rollen für Classic AWS WAF

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November

2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

AWS WAF Classic verwendet AWS Identity and Access Management (IAM) [serviceverknüpfte Rollen](#). Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, die direkt mit Classic verknüpft ist. AWS WAF Servicebezogene Rollen sind von AWS WAF Classic vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstverknüpfte Rolle erleichtert die Einrichtung von AWS WAF Classic, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS WAF Classic definiert die Berechtigungen seiner dienstbezogenen Rollen, und sofern nicht anders definiert, kann nur AWS WAF Classic diese Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann an keine andere IAM-Entität angefügt werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem die zugehörigen Ressourcen gelöscht wurden. Dadurch werden Ihre AWS WAF Classic-Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entfernen können.

Informationen zu anderen Services, die serviceverknüpften Rollen unterstützen, finden Sie unter [AWS -Services, die mit IAM funktionieren](#). Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Dienstbezogene Rollenberechtigungen für Classic AWS WAF

AWS WAF Classic verwendet die folgenden dienstbezogenen Rollen:

- `AWSServiceRoleForWAFLogging`
- `AWSServiceRoleForWAFRegionalLogging`

AWS WAF Classic verwendet diese serviceverknüpften Rollen, um Protokolle in Amazon Data Firehose zu schreiben. Diese Rollen werden nur verwendet, wenn Sie die Anmeldung aktivieren. AWS WAF Weitere Informationen finden Sie unter [Protokollieren von Web-ACL-Traffic-Informationen](#).

Die Rollen `AWSServiceRoleForWAFLogging` und die mit dem `AWSServiceRoleForWAFRegionalLogging` Dienst verknüpften Rollen vertrauen darauf, dass die folgenden Dienste (jeweils) die Rolle übernehmen:

- `waf.amazonaws.com`
`waf-regional.amazonaws.com`

Die Berechtigungsrichtlinien der Rollen ermöglichen es AWS WAF Classic, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: `firehose:PutRecord` und `firehose:PutRecordBatch` auf Amazon Data Firehose Datenstream-Ressourcen mit einem Namen, der mit "aws-waf-logs-" beginnt. z. B. `aws-waf-logs-us-east-2-analytics`.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [serviceverknüpfte Rollenberechtigungen](#) im IAM-Benutzerhandbuch.

Eine serviceverknüpfte Rolle für Classic erstellen AWS WAF

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie die AWS WAF Classic-Protokollierung auf der AWS Management Console aktivieren oder eine `PutLoggingConfiguration` Anfrage in der AWS WAF Classic CLI oder der AWS WAF Classic API stellen, erstellt AWS WAF Classic die serviceverknüpfte Rolle für Sie.

Sie müssen über die `iam:CreateServiceLinkedRole`-Berechtigung verfügen, um die Protokollierung zu aktivieren.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie die AWS WAF klassische Protokollierung aktivieren, erstellt AWS WAF Classic die serviceverknüpfte Rolle erneut für Sie.

Bearbeitung einer serviceverknüpften Rolle für Classic AWS WAF

AWS WAF In Classic können Sie die Rollen `AWSServiceRoleForWAFLogging` und die `AWSServiceRoleForWAFRegionalLogging` dienstbezogenen Rollen nicht bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach

der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer dienstverknüpften Rolle für Classic AWS WAF

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpften Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Note

Wenn der AWS WAF Classic-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um AWS WAF Classic-Ressourcen zu löschen, die von **AWSServiceRoleForWAFLogging** und verwendet werden **AWSServiceRoleForWAFRegionalLogging**

1. Entfernen Sie auf der AWS WAF Classic-Konsole die Protokollierung aus jeder Web-ACL. Weitere Informationen finden Sie unter [Protokollieren von Web-ACL-Traffic-Informationen](#).
2. Senden Sie über die API oder CLI eine `DeleteLoggingConfiguration`-Anforderung für jede Web-ACL, für die die Protokollierung aktiviert ist. Weitere Informationen finden Sie unter [AWS WAF Classic API Reference](#).

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die IAM-CLI oder die IAM-API, um die Rollen `AWSServiceRoleForWAFLogging` und `AWSServiceRoleForWAFRegionalLogging` die dienstverknüpften Rollen zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Leitfaden.

Unterstützte Regionen für serviceverknüpfte Classic-Rollen AWS WAF

AWS WAF Classic unterstützt im Folgenden die Verwendung von serviceverknüpften Rollen. AWS-Regionen

Name der Region	Region-ID	Support in AWS WAF Classic
USA Ost (Nord-Virginia)	us-east-1	Ja
USA Ost (Ohio)	us-east-2	Ja
USA West (Nordkalifornien)	us-west-1	Ja
USA West (Oregon)	us-west-2	Ja
Asien-Pazifik (Mumbai)	ap-south-1	Ja
Asien-Pazifik (Osaka)	ap-northeast-3	Ja
Asien-Pazifik (Seoul)	ap-northeast-2	Ja
Asien-Pazifik (Singapore)	ap-southeast-1	Ja
Asien-Pazifik (Sydney)	ap-southeast-2	Ja
Asien-Pazifik (Tokyo)	ap-northeast-1	Ja
Kanada (Zentral)	ca-central-1	Ja
Europa (Frankfurt)	eu-central-1	Ja
Europa (Irland)	eu-west-1	Ja
Europa (London)	eu-west-2	Ja
Europa (Paris)	eu-west-3	Ja
Südamerika (São Paulo)	sa-east-1	Ja

Protokollierung und Überwachung in AWS WAF Classic

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#).

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von AWS WAF Classic und Ihren AWS Lösungen. Sie sollten Überwachungsdaten aus allen Teilen Ihrer AWS Lösung sammeln, damit Sie einen etwaigen Ausfall an mehreren Stellen leichter debuggen können. AWS bietet mehrere Tools zur Überwachung Ihrer AWS WAF Classic-Ressourcen und zur Reaktion auf potenzielle Ereignisse:

CloudWatch Amazon-Alarme

Mithilfe von CloudWatch Alarmen beobachten Sie eine einzelne Metrik über einen von Ihnen festgelegten Zeitraum. Wenn die Metrik einen bestimmten Schwellenwert überschreitet, CloudWatch sendet eine Benachrichtigung an ein Amazon SNS SNS-Thema oder eine AWS Auto Scaling Richtlinie. Weitere Informationen finden Sie unter [Überwachung mit Amazon CloudWatch](#).

AWS CloudTrail Logs

CloudTrail bietet eine Aufzeichnung der Aktionen, die von einem Benutzer, einer Rolle oder einem AWS Dienst in AWS WAF Classic ausgeführt wurden. Anhand der von CloudTrail gesammelten Informationen können Sie die Anfrage an AWS WAF Classic, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln. Weitere Informationen finden Sie unter [Protokollierung von AWS CloudTrail-API-Aufrufen mit](#).

Konformitätsvalidierung für AWS WAF Classic

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#).

Informationen darüber, ob AWS-Service ein [AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt](#), finden Sie unter [Umfang nach Compliance-Programm AWS-Services unter](#) . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter [AWS Compliance-Programme AWS](#) .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter [Berichte herunterladen unter](#) .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- [Schnellstartanleitungen zu Sicherheit und Compliance](#) — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

Note

AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der [Referenz für HIPAA-berechtigte Services](#).

- [AWS Compliance-Ressourcen](#) — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- [AWS Leitfäden zur Einhaltung von Vorschriften für Kunden](#) — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- [Evaluierung von Ressourcen anhand von Regeln](#) im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- [AWS Security Hub](#)— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der [Security-Hub-Steuerungsreferenz](#).
- [AWS Audit Manager](#)— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz in AWS WAF Classic

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#).

Die AWS globale Infrastruktur basiert auf AWS-Regionen Availability Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter [AWS Globale](#) Infrastruktur.

Infrastruktursicherheit in AWS WAF Classic

Note

Dies ist die AWS WAF Classic-Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#).

Als verwalteter Dienst ist AWS WAF Classic durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter

[AWS Cloud-Sicherheit](#). Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf AWS WAF Classic zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit [AWS Security Token Service](#) (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

AWS WAF Klassische Kontingente

Note

Dies ist die AWS WAF klassische Dokumentation. Sie sollten diese Version nur verwenden, wenn Sie AWS WAF Ressourcen wie Regeln und Web-ACLs AWS WAF vor November 2019 erstellt und diese noch nicht auf die neueste Version migriert haben. Informationen zum Migrieren Ihrer Ressourcen finden Sie unter [Migrieren Sie Ihre AWS WAF Classic-Ressourcen zu AWS WAF](#).

Die neueste Version von AWS WAF finden Sie unter [AWS WAF](#)

AWS WAF Classic unterliegt den folgenden Kontingenten (früher als Limits bezeichnet).

AWS WAF Classic hat Standardkontingente für die Anzahl der Entitäten pro Konto und Region. Sie können [eine Erhöhung dieser Kontingente anfordern](#).

Ressource	Standardkontingent pro Konto und Region
Web-ACLs	50
Regeln	100
Rate-based-rules	5
Bedingungen pro Konto und Region	Für alle Bedingungen außer Regex-Match und Geo-Match 100 von jedem Bedingungstyp. Zum Beispiel 100 Größenbeschränkungsbedingungen und 100 IP-Übereinstimmungsbedingungen. Informationen zu Regex- und Geo-Match-Bedingungen finden Sie in der folgenden Tabelle.
Anforderungen pro Sekunde	25 000 pro Web-ACL*

*Dieses Kontingent gilt nur für AWS WAF Classic auf einem Application Load Balancer. [Die RPS-Kontingente \(Requests per Second\) für AWS WAF Classic on CloudFront entsprechen den unterstützten RPS-Kontingenten CloudFront, die im Entwicklerhandbuch beschrieben sind.](#)
[CloudFront](#)

Die folgenden Kontingente für AWS WAF Classic-Entitäten können nicht geändert werden.

Ressource	Kontingente pro Konto und Region
Regelgruppen je Web-ACL	2:1 vom Kunden erstellte Regelgruppe und 1 AWS Marketplace Regelgruppe
Regeln pro Web-ACL	10
Bedingungen pro Regel	10
IP-Adressbereiche (in CIDR-Notation) pro Bedingung für IP-Übereinstimmung	10.000 Sie können bis zu 1.000 Adressen gleichzeitig aktualisieren. Der API-Aufruf <code>UpdateIPSets</code> akzeptiert maximal 1.000 Adressen in einer einzigen Anfrage.
Nach der ratenbasierten Regel blockierte IP-Adressen	10.000

Ressource	Kontingente pro Konto und Region
Mindestgrenzwert der ratenbasierten Regel pro 5 Minuten	100
Filter pro Cross-Site-Scripting-Übereinstimmungsbedingung	10
Filter pro Größenbeschränkungsbedingung	10
Filter pro SQL Injection-Übereinstimmungsbedingung	10
Filter pro Bedingung für Zeichenfolgenübereinstimmung	10
Bei Zeichenfolgenabgleichsbedingungen die Anzahl der Zeichen in HTTP-Header-Namen, wenn Sie AWS WAF Classic so konfiguriert haben, dass die Header in Webanfragen auf einen bestimmten Wert überprüft werden	40
Bei Vergleichsbedingungen für Zeichenketten die Anzahl der Zeichen in dem Wert, nach denen AWS WAF Classic suchen soll	50
Regex-Abgleichbedingungen	10
Bei Regex-Abgleichbedingungen die Anzahl der Zeichen im Muster, nach denen Classic suchen soll AWS WAF	70
In Regex-Übereinstimmungsbedingungen ist die Anzahl der Muster pro Mustersatz festgelegt	10
In Regex-Übereinstimmungsbedingungen, die Anzahl der Mustersätze pro Regex-Bedingung	1
Mustersätze	5
Geo-Match-Bedingungen	50
Standorte je nach Geo-Match-Bedingung	50

AWS WAF Classic hat die folgenden festen Kontingente für Anrufe pro Konto und Region. Diese Kontingente gelten für die Gesamtzahl der Aufrufe des Dienstes über alle verfügbaren Mittel,

einschließlich der Konsole, CLI AWS CloudFormation, REST-API und SDKs. Diese Kontingente können nicht geändert werden.

Art des Anrufs	Kontingente pro Konto und Region
Maximale Anzahl von Aufrufen an AssociateWebACL	1 Anfrage alle 2 Sekunden
Maximale Anzahl von Aufrufen an DisassociateWebACL	1 Anfrage alle 2 Sekunden
Maximale Anzahl von Aufrufen an GetWebACLForResource	1 Anfrage pro Sekunde
Maximale Anzahl von Aufrufen an ListResourcesForWebACL	1 Anfrage pro Sekunde
Maximale Anzahl von Aufrufen an CreateWebACLMigrationStack	1 Anfrage pro Sekunde
Maximale Anzahl von Aufrufen an GetChangeToken	10 Anforderungen pro Sekunde
Maximale Anzahl von Aufrufen an GetChangeTokenStatus	1 Anfrage pro Sekunde
Maximale Anzahl von Aufrufen einer einzelnen List-Aktion, wenn kein anderes Kontingent dafür definiert ist	5 Anforderungen pro Sekunde
Maximale Anzahl von Aufrufen einer einzelnen Create-, Put-, Get- oder Update-Aktion, wenn kein anderes Kontingent dafür definiert ist	1 Anfrage pro Sekunde

AWS Shield

Der Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) ist für Ihre mit dem Internet verbundenen Anwendungen von größter Bedeutung. Wenn Sie Ihre Anwendung darauf aufbauen AWS, können Sie Schutzmaßnahmen nutzen, die diese ohne zusätzliche Kosten AWS bieten. Darüber hinaus können Sie den AWS Shield Advanced Managed Threat Protection Service verwenden, um Ihre Sicherheitslage durch zusätzliche Funktionen zur Erkennung, Abwehr und Reaktion auf DDoS-Angriffe zu verbessern.

AWS ist bestrebt, Ihnen die Tools, Best Practices und Services zur Verfügung zu stellen, mit denen Sie hohe Verfügbarkeit, Sicherheit und Widerstandsfähigkeit bei der Abwehr bösartiger Akteure im Internet gewährleisten können. Dieser Leitfaden soll IT-Entscheidungsträgern und Sicherheitsingenieuren helfen, zu verstehen, wie sie Shield und Shield Advanced verwenden können, um ihre Anwendungen besser vor DDoS-Angriffen und anderen externen Bedrohungen zu schützen.

Wenn Sie Ihre Anwendung darauf aufbauen AWS, erhalten Sie automatischen Schutz AWS vor gängigen volumetrischen DDoS-Angriffsvektoren wie UDP-Reflection-Angriffen und TCP-SYN-Floods. Sie können diese Schutzmaßnahmen nutzen, um die Verfügbarkeit der Anwendungen sicherzustellen, auf denen Sie ausgeführt werden, AWS indem Sie Ihre Architektur für DDoS-Resilienz entwerfen und konfigurieren.

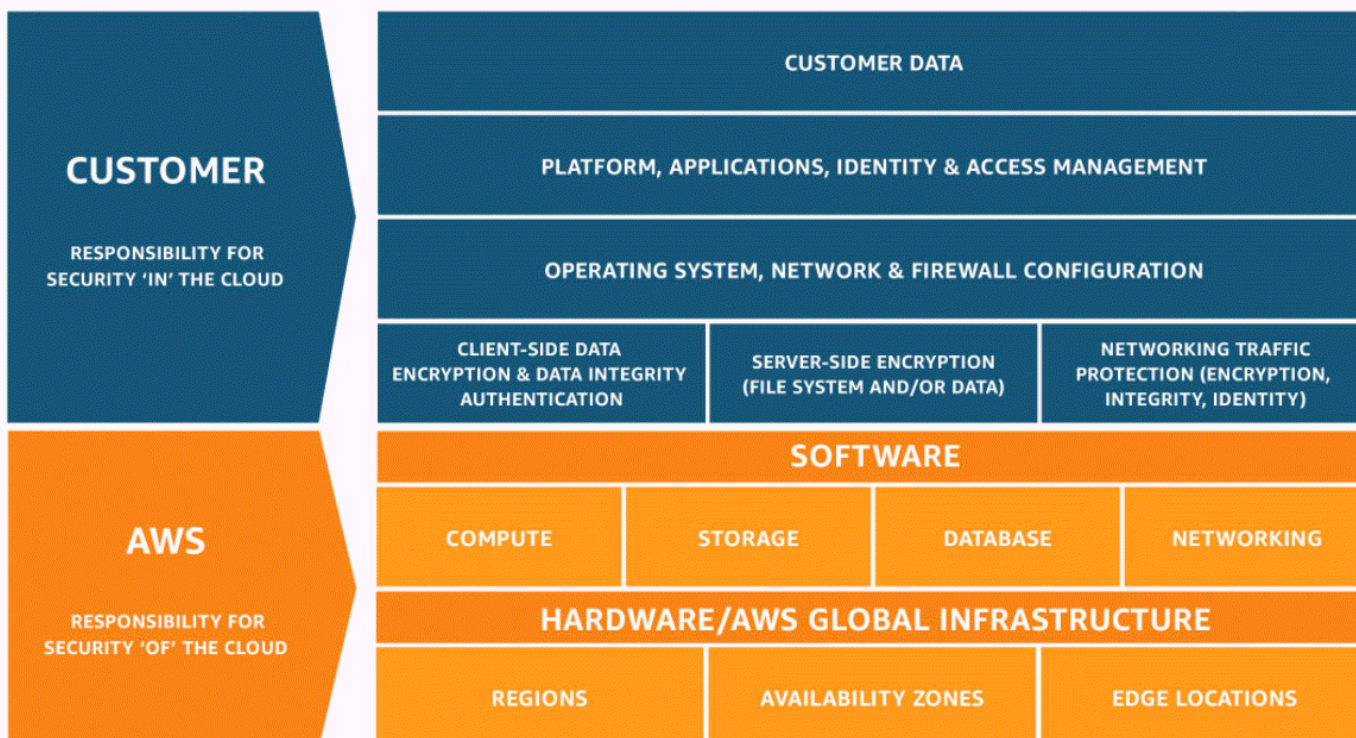
Dieser Leitfaden enthält Empfehlungen, die Ihnen helfen können, Ihre Anwendungsarchitekturen für DDoS-Resilienz zu entwerfen, zu erstellen und zu konfigurieren. Anwendungen, die sich an die in diesem Leitfaden aufgeführten Best Practices halten, können von einer verbesserten Kontinuität der Verfügbarkeit profitieren, wenn sie von größeren DDoS-Angriffen und einer breiteren Palette von DDoS-Angriffsvektoren betroffen sind. Darüber hinaus zeigt Ihnen dieser Leitfaden, wie Sie Shield Advanced verwenden, um einen optimierten DDoS-Schutz für Ihre kritischen Anwendungen zu implementieren. Dazu gehören Anwendungen, für die Sie Ihren Kunden ein gewisses Maß an Verfügbarkeit garantiert haben, und Anwendungen, für die Sie AWS bei DDoS-Ereignissen Betriebsunterstützung benötigen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Die Wirksamkeit unserer Sicherheitsfunktionen wird regelmäßig von externen Prüfern im Rahmen des [AWS -Compliance-Programms getestet und überprüft](#). Weitere

Informationen zu den Compliance-Programmen, die für Shield Advanced gelten, finden Sie unter [AWS Services im Umfang nach Compliance-Programmen](#).

- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. In Ihre Verantwortung fallen außerdem weitere Faktoren, wie z. B. die Vertraulichkeit der Daten, die Anforderungen Ihrer Organisation sowie geltende Gesetze und Vorschriften.



So funktionieren AWS Shield und Shield Advanced

AWS Shield Standard und AWS Shield Advanced bieten Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für AWS Ressourcen auf der Netzwerk- und Transportebene (Schicht 3 und 4) sowie auf der Anwendungsebene (Schicht 7). Ein DDoS-Angriff ist ein Angriff, bei dem mehrere kompromittierte Systeme versuchen, ein Ziel mit Datenverkehr zu überfluten. Ein DDoS-Angriff kann legitime Endbenutzer am Zugriff auf die Zieldienste hindern und das Ziel aufgrund des überwältigenden Datenverkehrs zum Absturz bringen.

AWS Shield bietet Schutz vor einer Vielzahl bekannter DDoS-Angriffsvektoren und Zero-Day-Angriffsvektoren. Shield Detection and Mitigation wurde entwickelt, um Bedrohungen abzuwehren, auch wenn sie dem Dienst zum Zeitpunkt der Entdeckung nicht ausdrücklich bekannt waren. Shield Standard wird automatisch und ohne Aufpreis bereitgestellt, wenn Sie es verwenden AWS.

Zu den Kategorien von Angriffen, die Shield erkennt, gehören:

- **Volumetrische Netzwerkangriffe (Schicht 3)** — Dies ist eine Unterkategorie von Angriffsvektoren auf Infrastrukturebene. Diese Vektoren versuchen, die Kapazität des Zielnetzwerks oder der Zielressource zu überlasten, um legitimen Benutzern den Dienst zu verweigern.
- **Netzwerkprotokollangriffe (Schicht 4)** — Dies ist eine Unterkategorie von Angriffsvektoren auf Infrastrukturebene. Diese Vektoren missbrauchen ein Protokoll, um der Zielressource den Zugriff zu verweigern. Ein häufiges Beispiel für einen Netzwerkprotokollangriff ist eine TCP-SYN-Flood, die den Verbindungsstatus von Ressourcen wie Servern, Load Balancern oder Firewalls erschöpfen kann. Ein Netzwerkprotokollangriff kann auch volumetrisch sein. Eine größere TCP-SYN-Flut könnte beispielsweise darauf abzielen, die Kapazität eines Netzwerks zu überlasten und gleichzeitig den Status der Zielressource oder der Zwischenressourcen zu erschöpfen.
- **Angriffe auf Anwendungsebene (Schicht 7)** — Diese Kategorie von Angriffsvektoren versucht, legitimen Benutzern den Dienst zu verweigern, indem eine Anwendung mit Abfragen überflutet wird, die für das Ziel gültig sind, wie z. B. Fluten von Webanfragen.

Inhalt

- [AWS Shield Standard Überblick](#)
- [AWS Shield Advanced Überblick](#)
 - [AWS Shield Advanced geschützte Ressourcen](#)
 - [AWS Shield Advanced Fähigkeiten und Optionen](#)
 - [Entscheidung, ob zusätzliche Schutzmaßnahmen abonniert AWS Shield Advanced und angewendet werden sollen](#)
- [Beispiele für DDoS-Angriffe](#)
- [Wie AWS Shield erkennt man Ereignisse](#)
 - [Erkennungslogik für Bedrohungen auf Infrastrukturebene](#)
 - [Erkennungslogik für Bedrohungen auf Anwendungsebene](#)
 - [Erkennungslogik für mehrere Ressourcen in einer Anwendung](#)
- [Wie AWS Shield mindert man Ereignisse](#)
 - [Funktionen zur Schadensbegrenzung](#)
 - [AWS Shield Mitigationslogik für CloudFront und Route 53](#)
 - [AWS Shield Minderungslogik für Regionen AWS](#)
 - [AWS Shield Risikominderungslogik für AWS Global Accelerator Standardbeschleuniger](#)

- [AWS Shield Advanced Schadensbegrenzungslogik für Elastic IPs](#)
- [AWS Shield Advanced Schadensbegrenzungslogik für Webanwendungen](#)

AWS Shield Standard Überblick

AWS Shield ist ein verwalteter Dienst zum Schutz vor Bedrohungen, der den Perimeter Ihrer Anwendung schützt. Der Perimeter ist der erste Eintrittspunkt für Anwendungsdatenverkehr, der von außerhalb des AWS Netzwerks kommt.

Um zu ermitteln, wo sich Ihr Anwendungsperimeter befindet, sollten Sie berücksichtigen, wie Benutzer über das Internet auf Ihre Anwendung zugreifen. Wenn sich der erste Einstiegspunkt in einer AWS Region befindet, ist der Anwendungsperimeter Ihre Amazon Virtual Private Cloud (VPC). Wenn Benutzer über Amazon Route 53 zu Ihrer Anwendung weitergeleitet werden und zuerst über Amazon CloudFront oder auf die Anwendung zugreifen AWS Global Accelerator, beginnt der Anwendungsperimeter am Rand des AWS Netzwerks.

Shield bietet Vorteile bei der DDoS-Erkennung und -Abwehr für alle Anwendungen AWS, auf denen sie ausgeführt werden, aber die Entscheidungen, die Sie beim Entwurf Ihrer Anwendungsarchitektur treffen, wirken sich auf Ihre DDoS-Resilienz aus. DDoS-Resilienz ist die Fähigkeit Ihrer Anwendung, während eines Angriffs weiterhin innerhalb der erwarteten Parameter zu arbeiten.

Alle AWS Kunden profitieren ohne zusätzliche Kosten vom automatischen Schutz von Shield Standard. Shield Standard schützt vor den häufigsten und am häufigsten auftretenden DDoS-Angriffen auf Netzwerk- und Transportschicht, die auf Ihre Website oder Anwendungen abzielen. Shield Standard trägt zwar zum Schutz aller AWS Kunden bei, Sie profitieren jedoch besonders von Amazon Route 53-Hosting-Zonen, CloudFront Amazon-Distributionen und AWS Global Accelerator Standardbeschleunigern. Diese Ressourcen erhalten umfassenden Verfügbarkeitsschutz vor allen bekannten Angriffen auf Netzwerk- und Transportebene.

AWS Shield Advanced Überblick

AWS Shield Advanced ist ein verwalteter Service, mit dem Sie Ihre Anwendung vor externen Bedrohungen wie DDoS-Angriffen, volumetrischen Bots und Versuchen, Sicherheitslücken auszunutzen, schützen können. Für einen höheren Schutz vor Angriffen können Sie AWS Shield Advanced abonnieren.

Wenn Sie Shield Advanced abonnieren und Ihre Ressourcen schützen, bietet Shield Advanced erweiterten Schutz vor DDoS-Angriffen für diese Ressourcen. Der Schutz, den Sie von Shield

Advanced erhalten, kann je nach Architektur und Konfiguration variieren. Verwenden Sie die Informationen in diesem Handbuch, um robuste Anwendungen mit Shield Advanced zu erstellen und zu schützen und um zu eskalieren, wenn Sie Hilfe von Experten benötigen.

Shield Advanced-Abonnements und AWS WAF Kosten

Ihr Shield Advanced-Abonnement deckt die Kosten für die Nutzung von AWS WAF Standardfunktionen für Ressourcen ab, die Sie mit Shield Advanced schützen. Die AWS WAF Standardgebühren, die durch Ihre Shield Advanced-Schutzmaßnahmen abgedeckt werden, sind die Kosten pro Web-ACL, die Kosten pro Regel und der Grundpreis pro Million Anfragen für die Prüfung von Webanfragen, bis zu 1.500 WCUs und bis zur Standardkörpergröße.

Durch die Aktivierung der automatischen DDoS-Abwehr auf Anwendungsebene von Shield Advanced wird Ihrer Web-ACL eine Regelgruppe hinzugefügt, die 150 Web-ACL-Kapazitätseinheiten (WCUs) verwendet. Diese WCUs werden auf die WCU-Nutzung in Ihrer Web-ACL angerechnet. Weitere Informationen finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#), [Die Shield Advanced-Regelgruppe](#) und [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#).

Ihr Abonnement AWS WAF für Shield Advanced deckt nicht die Nutzung von Ressourcen ab, die Sie nicht mit Shield Advanced schützen. Es deckt auch keine zusätzlichen, nicht standardmäßigen AWS WAF Kosten für geschützte Ressourcen ab. Beispiele für nicht standardmäßige AWS WAF Kosten sind die Kosten für Bot-Kontrolle, für CAPTCHA Regelaktionen, für Web-ACLs, die mehr als 1.500 WCUs verwenden, und für die Überprüfung des Anforderungstexts, der über die Standardgröße hinausgeht. Die vollständige Liste finden Sie auf der Seite mit den Preisen. AWS WAF

Vollständige Informationen und Preisbeispiele finden Sie unter [Shield Pricing](#) and [AWS WAF Pricing](#).

Abrechnung des Shield Advanced-Abonnements

Wenn Sie ein AWS Channel-Wiederverkäufer sind, wenden Sie sich an Ihr Account-Team, um Informationen und Beratung zu erhalten. Diese Rechnungsinformationen gelten für Kunden, die keine AWS Channel-Wiederverkäufer sind.

Für alle anderen gelten die folgenden Abonnement- und Abrechnungsrichtlinien:

- Bei Konten, die Mitglieder einer AWS Organizations Organisation sind, werden die Shield Advanced-Abonnements mit dem Zahlerkonto der Organisation in AWS Rechnung gestellt, unabhängig davon, ob das Zahlerkonto selbst abonniert ist.

- Wenn Sie mehrere Konten abonnieren, die sich in derselben [Kontenfamilie mit AWS Organizations konsolidierter Abrechnung](#) befinden, deckt ein Abonnementpreis alle abonnierten Konten in der Familie ab. Die Organisation muss Eigentümer all ihrer Ressourcen sein. AWS-Konten
- Wenn Sie mehrere Konten für mehrere Organisationen abonnieren, können Sie trotzdem eine Abonnementgebühr für alle Organisationen, Konten und Ressourcen zahlen, vorausgesetzt, Sie besitzen alle Konten. Wenden Sie sich an Ihren Kundenbetreuer oder AWS Support und beantragen Sie eine Gebührenbefreiung der AWS Shield Advanced Abonnementgebühren für alle Organisationen außer einer.

Detaillierte Preisinformationen und Beispiele finden Sie unter [AWS Shield Preisgestaltung](#).

Themen

- [AWS Shield Advanced geschützte Ressourcen](#)
- [AWS Shield Advanced Fähigkeiten und Optionen](#)
- [Entscheidung, ob zusätzliche Schutzmaßnahmen abonniert AWS Shield Advanced und angewendet werden sollen](#)

AWS Shield Advanced geschützte Ressourcen

Note

Shield Advanced-Schutzmaßnahmen sind nur für Ressourcen aktiviert, die Sie ausdrücklich in Shield Advanced angegeben haben oder die Sie durch eine AWS Firewall Manager Shield Advanced-Richtlinie schützen. Shield Advanced schützt Ihre Ressourcen nicht automatisch.

Sie können Shield Advanced für erweiterte Überwachung und Schutz mit den folgenden Ressourcentypen verwenden:

- CloudFront Amazon-Distributionen. Für CloudFront eine kontinuierliche Bereitstellung schützt Shield Advanced jede Staging-Distribution, die einer geschützten Primärdistribution zugeordnet ist.
- Gehostete Zonen von Amazon Route 53.
- AWS Global Accelerator Standardbeschleuniger.
- Amazon EC2 Elastic IP-Adressen. Shield Advanced schützt die Ressourcen, die geschützten Elastic IP-Adressen zugeordnet sind.

- Amazon EC2-Instances durch Zuordnung zu Amazon EC2 Elastic IP-Adressen.
- Die folgenden Elastic Load Balancing (ELB) -Load Balancer:
 - Load Balancer für Anwendungen.
 - Classic Load Balancer.
 - Network Load Balancers über Verknüpfungen zu Amazon EC2 Elastic IP-Adressen.

Weitere Informationen zum Schutz dieser Ressourcentypen finden Sie unter [AWS Shield Advanced Schutzmaßnahmen nach Ressourcentyp](#)

AWS Shield Advanced Fähigkeiten und Optionen

AWS Shield Advanced Das Abonnement umfasst die folgenden Funktionen und Optionen. Diese ergänzen die Funktionen zur DDoS-Erkennung und -Abwehr, die Sie bereits mit erhalten. AWS

- AWS WAF Integration — Shield Advanced verwendet AWS WAF Web-ACLs, Regeln und Regelgruppen als Teil seines Schutzes auf Anwendungsebene. Weitere Informationen zu finden Sie AWS WAF unter [Wie AWS WAF funktioniert](#)

Note

Ihr Shield Advanced-Abonnement deckt die Kosten für die Nutzung von AWS WAF Standardfunktionen für Ressourcen ab, die Sie mit Shield Advanced schützen. Die AWS WAF Standardgebühren, die durch Ihre Shield Advanced-Schutzmaßnahmen abgedeckt werden, sind die Kosten pro Web-ACL, die Kosten pro Regel und der Grundpreis pro Million Anfragen für die Prüfung von Webanfragen, bis zu 1.500 WCUs und bis zur Standardkörpergröße.

Durch die Aktivierung der automatischen DDoS-Abwehr auf Anwendungsebene von Shield Advanced wird Ihrer Web-ACL eine Regelgruppe hinzugefügt, die 150 Web-ACL-Kapazitätseinheiten (WCUs) verwendet. Diese WCUs werden auf die WCU-Nutzung in Ihrer Web-ACL angerechnet. Weitere Informationen finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#), [Die Shield Advanced-Regelgruppe](#) und [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#).

Ihr Abonnement AWS WAF für Shield Advanced deckt nicht die Nutzung von Ressourcen ab, die Sie nicht mit Shield Advanced schützen. Es deckt auch keine zusätzlichen, nicht standardmäßigen AWS WAF Kosten für geschützte Ressourcen ab. Beispiele für nicht standardmäßige AWS WAF Kosten sind die Kosten für Bot-Kontrolle, für CAPTCHA Regelaktionen, für Web-ACLs, die mehr als 1.500 WCUs verwenden, und

für die Überprüfung des Anforderungstexts, der über die Standardgröße hinausgeht. Die vollständige Liste finden Sie auf der Seite mit den Preisen. AWS WAF Vollständige Informationen und Preisbeispiele finden Sie unter [Shield Pricing](#) and [AWS WAF Pricing](#).

- Automatische DDoS-Abwehr auf Anwendungsebene — Sie können Shield Advanced so konfigurieren, dass es automatisch reagiert, um Angriffe auf Anwendungsebene (Schicht 7) auf Ihre geschützten Ressourcen abzuwehren. Mit automatischer Abwehr erzwingt Shield Advanced eine AWS WAF Ratenbegrenzung für Anfragen von bekannten DDoS-Quellen und fügt als Reaktion auf erkannte DDoS-Angriffe automatisch benutzerdefinierte AWS WAF Schutzmaßnahmen hinzu und verwaltet diese. Sie können die automatische Abwehr so konfigurieren, dass die Webanfragen, die Teil eines Angriffs sind, gezählt oder blockiert werden.

Weitere Informationen finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#).

- Gesundheitsbasierte Erkennung — Sie können Amazon Route 53-Zustandsprüfungen mit Shield Advanced als Grundlage für die Erkennung und Abwehr von Ereignissen verwenden. Health Checks überwachen Ihre Anwendung gemäß Ihren Spezifikationen und melden fehlerfrei, wenn Ihre Spezifikationen erfüllt werden, und ungesund, wenn dies nicht der Fall ist. Die Verwendung von Integritätsprüfungen mit Shield Advanced hilft dabei, Fehlalarme zu verhindern und ermöglicht eine schnellere Erkennung und Abwehr, wenn eine geschützte Ressource fehlerhaft ist. Sie können die zustandsbasierte Erkennung für jeden Ressourcentyp außer für gehostete Route 53-Zonen verwenden. Shield Advanced Proactive Engagement ist nur für Ressourcen verfügbar, für die die gesundheitsbasierte Erkennung aktiviert ist.

Weitere Informationen finden Sie unter [Gesundheitsbasierte Erkennung mithilfe von Gesundheitschecks](#).

- Schutzgruppen — Sie können Schutzgruppen verwenden, um logische Gruppierungen Ihrer geschützten Ressourcen zu erstellen, um die gesamte Gruppe besser erkennen und abwehren zu können. Sie können die Kriterien für die Mitgliedschaft in einer Schutzgruppe so definieren, dass neu geschützte Ressourcen automatisch berücksichtigt werden. Eine geschützte Ressource kann mehreren Schutzgruppen angehören.

Weitere Informationen finden Sie unter [AWS Shield Advanced Schutzgruppen](#).

- Verbesserter Einblick in DDoS-Ereignisse und -Angriffe — Shield Advanced bietet Ihnen Zugriff auf erweiterte Echtzeit-Metriken und Berichte für einen umfassenden Einblick in Ereignisse und

Angriffe auf Ihre geschützten AWS Ressourcen. Sie können über die Shield Advanced-API und -Konsole sowie über CloudWatch Amazon-Metriken auf diese Informationen zugreifen.

Weitere Informationen finden Sie unter [Einblick in DDoS-Ereignisse](#).

- Zentralisierte Verwaltung der Shield Advanced-Schutzmaßnahmen von AWS Firewall Manager — Sie können den Firewall Manager verwenden, um den Shield Advanced-Schutz automatisch auf Ihre neuen Konten und Ressourcen anzuwenden und AWS WAF Regeln für Ihre Web-ACLs bereitzustellen. Die Shield Advanced-Schutzrichtlinien von Firewall Manager sind für Shield Advanced-Kunden ohne zusätzliche Kosten enthalten. Sie können Ihre Shield Advanced-Überwachungsaktivitäten für Ihre Konten auch zentralisieren, indem Sie den Firewall Manager mit einem Amazon Simple Notification Service (SNS) -Thema oder verwenden. AWS Security Hub

Weitere Informationen zur Verwendung von Firewall Manager zur Verwaltung von Shield Advanced-Schutzmaßnahmen finden Sie unter [AWS Firewall Manager](#) und [AWS Shield Advanced Richtlinien](#). Informationen zu den Preisen von Firewall Manager finden Sie unter [AWS Firewall Manager Preise](#).

- AWS Shield Response Team (SRT) — Das SRT verfügt über umfangreiche Erfahrung im Schutz AWS von Amazon.com und seinen Tochtergesellschaften. Als AWS Shield Advanced Kunde können Sie sich jederzeit an das SRT wenden, um Unterstützung bei einem DDoS-Angriff zu erhalten, der die Verfügbarkeit Ihrer Anwendung beeinträchtigt. Sie können auch mit dem SRT zusammenarbeiten, um benutzerdefinierte Schutzmaßnahmen für Ihre Ressourcen zu erstellen und zu verwalten. Um die Dienste des SRT nutzen zu können, müssen Sie auch den [Business Support Plan oder den Enterprise Support Plan](#) abonniert haben.

Weitere Informationen finden Sie unter [Unterstützung durch das Shield Response Team \(SRT\)](#).

- Proaktives Engagement — Bei proaktivem Engagement kontaktiert Sie das Shield Response Team (SRT) direkt, wenn die Amazon Route 53-Zustandsprüfung, die Sie mit Ihrer geschützten Ressource verknüpft haben, während eines von Shield Advanced erkannten Ereignisses fehlerhaft wird. Auf diese Weise können Sie schneller mit Experten in Kontakt treten, wenn die Verfügbarkeit Ihrer Anwendung durch einen vermuteten Angriff beeinträchtigt werden könnte.

Weitere Informationen finden Sie unter [Konfiguration von proaktivem Engagement](#).

- Möglichkeiten zum Kostenschutz — Shield Advanced bietet einen gewissen Kostenschutz vor hohen Kosten, AWS die durch einen DDoS-Angriff auf Ihre geschützten Ressourcen entstehen könnten. Dies kann die Deckung von Spitzenwerten bei den Gebühren für die ausgehende Datenübertragung (DTO) von Shield Advanced beinhalten. Shield Advanced bietet jeglichen Kostenschutz in Form von Shield Advanced-Servicegutschriften.

Weitere Informationen finden Sie unter [Eine Gutschrift beantragen in AWS Shield Advanced](#).

Entscheidung, ob zusätzliche Schutzmaßnahmen abonniert AWS Shield Advanced und angewendet werden sollen

Sehen Sie sich die Szenarien in diesem Abschnitt an, um zu entscheiden, welche Konten Sie abonnieren AWS Shield Advanced und wo zusätzliche Schutzmaßnahmen angewendet werden sollten. Mit Shield Advanced zahlen Sie eine monatliche Abonnementgebühr für alle Konten, die unter einem konsolidierten Rechnungskonto erstellt wurden, zuzüglich Nutzungsgebühren, die auf den übertragenen GB an Daten basieren. Informationen zu den Preisen von Shield Advanced finden Sie unter [AWS Shield Advanced Preise](#).

Um eine Anwendung und ihre Ressourcen mit Shield Advanced zu schützen, abonnieren Sie Shield Advanced für die Konten, die die Anwendung verwalten, und fügen dann Schutzmaßnahmen zu den Ressourcen der Anwendung hinzu. Informationen zum Abonnieren von Konten und zum Schutz von Ressourcen finden Sie unter [Erste Schritte mit AWS Shield Advanced](#)

Shield Advanced-Abonnements und AWS WAF Kosten

Ihr Shield Advanced-Abonnement deckt die Kosten für die Nutzung von AWS WAF Standardfunktionen für Ressourcen ab, die Sie mit Shield Advanced schützen. Die AWS WAF Standardgebühren, die durch Ihre Shield Advanced-Schutzmaßnahmen abgedeckt werden, sind die Kosten pro Web-ACL, die Kosten pro Regel und der Grundpreis pro Million Anfragen für die Prüfung von Webanfragen, bis zu 1.500 WCUs und bis zur Standardkörpergröße.

Durch die Aktivierung der automatischen DDoS-Abwehr auf Anwendungsebene von Shield Advanced wird Ihrer Web-ACL eine Regelgruppe hinzugefügt, die 150 Web-ACL-Kapazitätseinheiten (WCUs) verwendet. Diese WCUs werden auf die WCU-Nutzung in Ihrer Web-ACL angerechnet. Weitere Informationen finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#), [Die Shield Advanced-Regelgruppe](#) und [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#).

Ihr Abonnement AWS WAF für Shield Advanced deckt nicht die Nutzung von Ressourcen ab, die Sie nicht mit Shield Advanced schützen. Es deckt auch keine zusätzlichen, nicht standardmäßigen AWS WAF Kosten für geschützte Ressourcen ab. Beispiele für nicht standardmäßige AWS WAF Kosten sind die Kosten für Bot-Kontrolle, für CAPTCHA Regelaktionen, für Web-ACLs, die mehr als 1.500 WCUs verwenden, und für die Überprüfung des Anforderungstexts, der über die Standardgröße hinausgeht. Die vollständige Liste finden Sie auf der Seite mit den Preisen. AWS WAF

Vollständige Informationen und Preisbeispiele finden Sie unter [Shield Pricing](#) and [AWS WAF Pricing](#).

Abrechnung des Shield Advanced-Abonnements

Wenn Sie ein AWS Channel-Wiederverkäufer sind, wenden Sie sich an Ihr Account-Team, um Informationen und Beratung zu erhalten. Diese Rechnungsinformationen gelten für Kunden, die keine AWS Channel-Wiederverkäufer sind.

Für alle anderen gelten die folgenden Abonnement- und Abrechnungsrichtlinien:

- Bei Konten, die Mitglieder einer AWS Organizations Organisation sind, werden die Shield Advanced-Abonnements mit dem Zahlerkonto der Organisation in AWS Rechnung gestellt, unabhängig davon, ob das Zahlerkonto selbst abonniert ist.
- Wenn Sie mehrere Konten abonnieren, die sich in derselben [Kontenfamilie mit AWS Organizations konsolidierter Abrechnung](#) befinden, deckt ein Abonnementpreis alle abonnierten Konten in der Familie ab. Die Organisation muss Eigentümer all ihrer Ressourcen sein. AWS-Konten
- Wenn Sie mehrere Konten für mehrere Organisationen abonnieren, können Sie trotzdem eine Abonnementgebühr für alle Organisationen, Konten und Ressourcen zahlen, vorausgesetzt, Sie besitzen alle Konten. Wenden Sie sich an Ihren Kundenbetreuer oder AWS Support und beantragen Sie eine Gebührenbefreiung der AWS Shield Advanced Abonnementgebühren für alle Organisationen außer einer.

Detaillierte Preisinformationen und Beispiele finden Sie unter [AWS Shield Preisgestaltung](#).

Identifizierung der zu schützenden Anwendungen

Erwägen Sie die Implementierung von Shield Advanced-Schutzmaßnahmen für Anwendungen, für die Sie Folgendes benötigen:

- Garantierte Verfügbarkeit für die Benutzer der Anwendung.
- Schneller Zugang zu Experten für DDoS-Abwehr, falls die Anwendung von einem DDoS-Angriff betroffen ist.
- Kenntnis der Tatsache AWS , dass die Anwendung von einem DDoS-Angriff betroffen sein könnte, und Benachrichtigung Ihrer Sicherheits- oder Betriebsteams über Angriffe AWS und deren Eskalation.
- Vorhersehbarkeit Ihrer Cloud-Kosten, auch wenn sich ein DDoS-Angriff auf Ihre Nutzung von Diensten auswirkt. AWS

Wenn eine Anwendung oder ihre Ressourcen eines der oben genannten Dinge erfordern, sollten Sie in Erwägung ziehen, Abonnements für die entsprechenden Konten zu erstellen.

Identifizieren der zu schützenden Ressourcen

Erwägen Sie, für jedes abonnierte Konto jeder Ressource, die eines der folgenden Merkmale aufweist, einen Shield Advanced-Schutz hinzuzufügen:

- Die Ressource dient externen Benutzern im Internet.
- Die Ressource ist im Internet verfügbar und ist auch Teil einer kritischen Anwendung. Berücksichtigen Sie jede gefährdete Ressource, unabhängig davon, ob Sie beabsichtigen, dass Benutzer im Internet auf sie zugreifen.
- Die Ressource ist durch eine AWS WAF Web-ACL geschützt.

Weitere Informationen zum Erstellen und Verwalten von Schutzmaßnahmen für Ihre Ressourcen finden Sie unter [Ressourcenschutz in AWS Shield Advanced](#).

Folgen Sie außerdem den Empfehlungen in diesem Leitfaden, um sicherzustellen, dass Sie Ihre Anwendung auf DDoS-Resilienz ausrichten und dass Sie die Funktionen von Shield Advanced für optimalen Schutz ordnungsgemäß konfiguriert haben.

Beispiele für DDoS-Angriffe

AWS Shield Advanced bietet erweiterten Schutz vor vielen Arten von Angriffen.

In der folgenden Liste werden einige gängige Angriffsarten beschrieben:

User Datagram Protocol (UDP) Reflection-Angriff

Bei UDP-Reflection-Angriffen kann ein Angreifer die Quelle einer Anfrage fälschen und UDP verwenden, um eine umfangreiche Antwort vom Server auszulösen. Der zusätzliche Netzwerkverkehr, der auf die gefälschte, angegriffene IP-Adresse gerichtet ist, kann den Zielserver verlangsamen und legitime Endbenutzer daran hindern, auf die benötigten Ressourcen zuzugreifen.

TCP-SYN-Flut

Die Absicht eines TCP-SYN-Flood-Angriffs besteht darin, die verfügbaren Ressourcen eines Systems zu erschöpfen, indem Verbindungen in einem halboffenen Zustand belassen werden. Wenn ein Benutzer eine Verbindung zu einem TCP-Dienst wie einem Webserver herstellt,

sendet der Client ein TCP-SYN-Paket. Der Server sendet eine Bestätigung und der Client sendet ebenfalls eine eigene Bestätigung – damit ist der "Dreibege-Handshake" komplett. Bei einer TCP-SYN-Flood wird die dritte Bestätigung nie zurückgegeben, und der Server wartet auf eine Antwort. Dies kann verhindern, dass andere Benutzer eine Verbindung zum Server aufbauen.

DNS Query Flood-Angriff

Bei einer DNS-Abfrageflut verwendet ein Angreifer mehrere DNS-Abfragen, um die Ressourcen eines DNS-Servers zu erschöpfen. AWS Shield Advanced kann dazu beitragen, Schutz vor DNS-Query-Flood-Angriffen auf Route 53-DNS-Server zu bieten.

HTTP Flood/Cache-Busting-Angriff (Layer 7)

Bei einer HTTP-Flut, einschließlich GET und POST Floods, sendet ein Angreifer mehrere HTTP-Anfragen, die anscheinend von einem echten Benutzer der Webanwendung stammen. Cache-Busting-Angriffe zählen zu den HTTP Flood-Angriffen. Sie nutzen Abweichungen in der Abfragezeichenfolge der HTTP-Anforderung, damit die Inhalte nicht aus dem Cache eines Edge-Standorts gelesen werden, und erzwingen so den Inhaltsabruf vom ursprünglichen Webserver. Das wiederum sorgt für eine erhöhte und potenziell schädliche Auslastung des ursprünglichen Webservers.

Wie AWS Shield erkennt man Ereignisse

AWS betreibt Service-Level-Erkennungssysteme für das AWS Netzwerk und einzelne AWS Dienste, um sicherzustellen, dass diese auch während eines DDoS-Angriffs verfügbar bleiben. Darüber hinaus überwachen Erkennungssysteme auf Ressourcenebene jede einzelne AWS Ressource, um sicherzustellen, dass der Datenverkehr zu der Ressource innerhalb der erwarteten Parameter bleibt. Diese Kombination schützt sowohl die AWS Zielressource als auch die AWS Dienste, indem Schutzmaßnahmen angewendet werden, die bekannte schädliche Pakete verwerfen, potenziell bösartigen Datenverkehr hervorheben und den Datenverkehr von Endbenutzern priorisieren.

Entdeckte Ereignisse erscheinen in Ihren Shield Advanced-Ereigniszusammenfassungen, Angriffsdetails und CloudWatch Amazon-Metriken entweder als Name des DDoS-Angriffsvektors oder als `Volumetric` ob die Bewertung auf dem Verkehrsvolumen statt auf der Signatur basieren würde. Weitere Informationen zu den Dimensionen des Angriffsvektors, die in der `DDoSDetected` CloudWatch Metrik verfügbar sind, finden Sie unter [AWS Shield Advanced Metriken](#)

Themen

- [Erkennungslogik für Bedrohungen auf Infrastrukturebene](#)

- [Erkennungslogik für Bedrohungen auf Anwendungsebene](#)
- [Erkennungslogik für mehrere Ressourcen in einer Anwendung](#)

Erkennungslogik für Bedrohungen auf Infrastrukturebene

Die Erkennungslogik, die verwendet wird, um gezielte AWS Ressourcen vor DDoS-Angriffen in den Infrastrukturebenen (Schicht 3 und Schicht 4) zu schützen, hängt vom Ressourcentyp ab und davon, ob die Ressource geschützt ist. AWS Shield Advanced

Erkennung für Amazon CloudFront und Amazon Route 53

Wenn Sie Ihre Webanwendung mit CloudFront und Route 53 bereitstellen, werden alle Pakete an die Anwendung von einem vollständig integrierten DDoS-Abwehrsystem überprüft, das keine beobachtbare Latenz verursacht. DDoS-Angriffe auf CloudFront Distributionen und auf Route 53 gehostete Zonen werden in Echtzeit abgewehrt. Diese Schutzmaßnahmen gelten unabhängig davon, ob Sie sie verwenden. AWS Shield Advanced

Verwenden CloudFront Sie nach Möglichkeit die bewährte Methode, Route 53 als Einstiegspunkt für Ihre Webanwendung zu verwenden, um DDoS-Ereignisse so schnell wie möglich zu erkennen und zu bekämpfen.

Erkennung für AWS Global Accelerator und regionale Dienste

Die Erkennung auf Ressourcenebene schützt AWS Global Accelerator Standardbeschleuniger und Ressourcen, die in AWS Regionen eingeführt werden, wie Classic Load Balancers, Application Load Balancers und Elastic IP-Adressen (EIPs). Diese Ressourcentypen werden im Hinblick auf Datenverkehrserhöhungen überwacht, die auf das Vorhandensein eines DDoS-Angriffs hinweisen könnten, für den eine Abwehr erforderlich ist. Jede Minute wird der Verkehr zu jeder AWS Ressource ausgewertet. Wenn der Verkehr zu einer Ressource erhöht ist, werden zusätzliche Prüfungen durchgeführt, um die Kapazität der Ressource zu messen.

Shield führt die folgenden Standardprüfungen durch:

- Amazon Elastic Compute Cloud (Amazon EC2) -Instances, EIPs, die an Amazon EC2 EC2-Instances angehängt sind — Shield ruft Kapazität von der geschützten Ressource ab. Die Kapazität hängt vom Instance-Typ, der Instance-Größe und anderen Faktoren des Ziels ab, z. B. davon, ob die Instance Enhanced Networking verwendet.
- Classic Load Balancers und Application Load Balancers — Shield ruft Kapazität vom Ziel-Load Balancer-Knoten ab.

- EIPs, die an Network Load Balancers angeschlossen sind — Shield ruft Kapazität vom Ziel-Load Balancer ab. Die Kapazität ist unabhängig von der Gruppenkonfiguration des Ziel-Load Balancers.
- AWS Global Accelerator Standardbeschleuniger — Shield ruft Kapazität ab, die auf der Endpunktkonfiguration basiert.

Diese Bewertungen beziehen sich auf mehrere Dimensionen des Netzwerkverkehrs, z. B. auf Port und Protokoll. Wenn die Kapazität der Zielressource überschritten wird, führt Shield eine DDoS-Abwehr durch. Die von Shield eingeführten Abhilfemaßnahmen werden den DDoS-Verkehr reduzieren, ihn aber möglicherweise nicht beseitigen. Shield kann auch Abhilfemaßnahmen ergreifen, wenn ein Bruchteil der Kapazität der Ressource bei einer Verkehrsdimension überschritten wird, die mit bekannten DDoS-Angriffsvektoren übereinstimmt. Shield gewährt dieser Abwehr eine begrenzte Gültigkeitsdauer (TTL), die verlängert wird, solange der Angriff andauert.

Note

Von Shield vorgenommene Abhilfemaßnahmen reduzieren den DDoS-Verkehr, verhindern ihn aber möglicherweise nicht. Sie können Shield um Lösungen wie AWS Network Firewall oder eine On-Host-Firewall erweitern, iptables um zu verhindern, dass Ihre Anwendung Datenverkehr verarbeitet, der für Ihre Anwendung nicht gültig ist oder nicht von legitimen Endbenutzern generiert wurde.

Die erweiterten Schutzmaßnahmen von Shield erweitern die bestehenden Shield-Erkennungsaktivitäten um Folgendes:

- Niedrigere Erkennungsschwellen — Shield Advanced legt Schutzmaßnahmen auf die Hälfte der berechneten Kapazität fest. Auf diese Weise können Angriffe, die langsam zunehmen, schneller abgewehrt und Angriffe, die eine mehrdeutigere volumetrische Signatur aufweisen, eingedämmt werden.
- Schutz vor intermittierenden Angriffen — Shield Advanced platziert Abhilfemaßnahmen mit einer exponentiell steigenden Gültigkeitsdauer (TTL), die auf der Häufigkeit und Dauer der Angriffe basiert. Dadurch bleiben die Abwehrmaßnahmen länger wirksam, wenn eine Ressource häufig angegriffen wird und wenn ein Angriff in kurzen Ausbrüchen erfolgt.
- Integritätsbasierte Erkennung — Wenn Sie eine Route 53-Zustandsprüfung mit einer geschützten Shield Advanced-Ressource verknüpfen, wird der Status der Integritätsprüfung in der Erkennungslogik verwendet. Wenn bei einem erkannten Ereignis die Integritätsprüfung fehlerfrei

ist, muss Shield Advanced erst dann darauf vertrauen, dass es sich bei dem Ereignis um einen Angriff handelt, bevor eine Abwehr eingeleitet wird. Wenn der Gesundheitscheck stattdessen fehlerhaft ist, kann Shield Advanced eine Abhilfemaßnahme vornehmen, noch bevor das Vertrauen hergestellt wurde. Diese Funktion hilft dabei, Fehlalarme zu vermeiden und ermöglicht schnellere Reaktionen auf Angriffe, die Ihre Anwendung betreffen. Informationen zu Integritätsprüfungen mit Shield Advanced finden Sie unter [Gesundheitsbasierte Erkennung mithilfe von Gesundheitschecks](#).

Erkennungslogik für Bedrohungen auf Anwendungsebene

AWS Shield Advanced bietet die Erkennung von Webanwendungsebenen für geschützte CloudFront Amazon-Distributionen und Application Load Balancers. Wenn Sie diese Ressourcentypen mit Shield Advanced schützen, können Sie Ihrem Schutz eine AWS WAF Web-ACL zuordnen, um die Erkennung der Webanwendungsebene zu aktivieren. Shield Advanced verwendet Anforderungsdaten für die zugehörige Web-ACL und erstellt eine Datenverkehrsbasis für Ihre Anwendung. Die Erkennung von Webanwendungsebenen basiert auf der nativen Integration zwischen Shield Advanced und AWS WAF. Weitere Informationen zum Schutz auf Anwendungsebene, einschließlich der Zuordnung einer AWS WAF Web-ACL zu einer geschützten Shield Advanced-Ressource, finden Sie unter [AWS Shield Advanced Schutzmaßnahmen auf Anwendungsebene \(Schicht 7\)](#)

Zur Erkennung von Webanwendungsebenen überwacht Shield Advanced den Anwendungsverkehr und vergleicht ihn mit historischen Ausgangsdaten, um nach Anomalien zu suchen. Diese Überwachung deckt das Gesamtvolumen und die Zusammensetzung des Datenverkehrs ab. Während eines DDoS-Angriffs gehen wir davon aus, dass sich sowohl das Volumen als auch die Zusammensetzung des Datenverkehrs ändern werden, und Shield Advanced verlangt bei beiden eine statistisch signifikante Abweichung, um ein Ereignis zu deklarieren.

Shield Advanced führt seine Messungen anhand historischer Zeitfenster durch. Dieser Ansatz reduziert Fehlmeldungen aufgrund legitimer Änderungen des Verkehrsaufkommens oder aufgrund von Änderungen des Datenverkehrs, die einem erwarteten Muster entsprechen, z. B. bei einem Verkauf, der jeden Tag zur gleichen Uhrzeit angeboten wird.

Note

Vermeiden Sie Fehlalarme in Ihren Shield Advanced-Schutzmaßnahmen, indem Sie Shield Advanced Zeit geben, Baselines zu erstellen, die normale, legitime Datenverkehrsmuster darstellen. Shield Advanced beginnt mit der Erfassung von Informationen für seine Baseline, wenn Sie Ihrer geschützten Ressource eine Web-ACL zuordnen. Ordnen Sie Ihrer geschützten Ressource mindestens 24 Stunden vor einem geplanten Ereignis, das zu

ungewöhnlichen Mustern im Webverkehr führen könnte, eine Web-ACL zu. Die Erkennung auf Webanwendungsebene von Shield Advanced ist am genauesten, wenn 30 Tage normalen Datenverkehrs beobachtet wurden.

Die Zeit, die Shield Advanced benötigt, um ein Ereignis zu erkennen, hängt davon ab, wie stark sich das Verkehrsaufkommen ändert. Bei Änderungen mit geringerem Volumen beobachtet Shield Advanced den Verkehr über einen längeren Zeitraum, um die Gewissheit zu stärken, dass ein Ereignis eintritt. Bei Änderungen mit höherer Lautstärke erkennt Shield Advanced ein Ereignis schneller und meldet es schneller.

Eine ratenbasierte Regel in Ihrer Web-ACL, unabhängig davon, ob sie von Ihnen oder durch die automatische Abwehr auf Anwendungsebene von Shield Advanced hinzugefügt wurde, kann einen Angriff abwehren, bevor er ein erkennbares Ausmaß erreicht. Weitere Informationen zur automatischen DDoS-Abwehr auf Anwendungsebene finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#)

Note

Sie können Ihre Anwendung so einrichten, dass sie bei erhöhtem Traffic oder hoher Auslastung skaliert wird, um sicherzustellen, dass sie nicht durch kleinere Anforderungsfluten beeinträchtigt wird. Mit Shield Advanced sind Ihre geschützten Ressourcen durch einen Kostenschutz abgedeckt. Dies schützt Sie vor unerwarteten Erhöhungen Ihrer Cloud-Rechnung, die als Folge eines DDoS-Angriffs auftreten könnten. Weitere Informationen zum Kostenschutz von Shield Advanced finden Sie unter [Eine Gutschrift beantragen in AWS Shield Advanced](#).

Erkennungslogik für mehrere Ressourcen in einer Anwendung

Sie können AWS Shield Advanced Schutzgruppen verwenden, um Sammlungen geschützter Ressourcen zu erstellen, die Teil derselben Anwendung sind. Sie können wählen, welche geschützten Ressourcen in einer Gruppe platziert werden sollen, oder angeben, dass alle Ressourcen desselben Typs als eine Gruppe behandelt werden sollen. Sie können beispielsweise eine Gruppe mit allen Application Load Balancern erstellen. Wenn Sie eine Schutzgruppe erstellen, aggregiert Shield Advanced Detection den gesamten Datenverkehr für die geschützten Ressourcen innerhalb der Gruppe. Dies ist nützlich, wenn Sie über viele Ressourcen verfügen, von denen jede eine geringe Menge an Datenverkehr, aber ein großes aggregiertes Volumen aufweist. Sie können

Schutzgruppen auch verwenden, um Anwendungsbasislinien beizubehalten, was bei blaugrünen Bereitstellungen der Fall ist, bei denen der Datenverkehr zwischen geschützten Ressourcen übertragen wird.

Sie können den Datenverkehr in Ihrer Schutzgruppe auf eine der folgenden Arten aggregieren:

- **Summe** — Diese Aggregation kombiniert den gesamten Datenverkehr zwischen den Ressourcen in der Schutzgruppe. Sie können diese Aggregation verwenden, um sicherzustellen, dass neu erstellte Ressourcen über eine bestehende Basislinie verfügen, und um die Erkennungsempfindlichkeit zu verringern, wodurch Fehlalarme vermieden werden können.
- **Mittelwert** — Bei dieser Aggregation wird der Durchschnitt des gesamten Datenverkehrs innerhalb der Schutzgruppe verwendet. Sie können diese Aggregation für Anwendungen verwenden, bei denen der Datenverkehr zwischen Ressourcen einheitlich ist, z. B. für Load Balancer.
- **Max** — Diese Aggregation verwendet den höchsten Traffic aller Ressourcen in der Schutzgruppe. Sie können diese Aggregation verwenden, wenn mehrere Ebenen einer Anwendung in einer Schutzgruppe vorhanden sind. Beispielsweise haben Sie möglicherweise eine Schutzgruppe, die eine CloudFront Distribution, ihren Application Load Balancer Ursprung und die Amazon EC2 EC2-Instance-Ziele des Application Load Balancers umfasst.

Sie können Schutzgruppen auch verwenden, um die Geschwindigkeit zu erhöhen, mit der Shield Advanced Abhilfemaßnahmen für Angriffe einsetzt, die auf mehrere mit dem Internet verbundene Elastic IPs oder AWS Global Accelerator Standardbeschleuniger abzielen. Wenn eine Ressource in einer Schutzgruppe ins Visier genommen wird, stellt Shield Advanced Vertrauen für die anderen Ressourcen in der Gruppe her. Dadurch wird die Erkennung von Shield Advanced in einen Alarmzustand versetzt und der Zeitaufwand für die Erstellung zusätzlicher Schutzmaßnahmen kann reduziert werden.

Weitere Informationen zu Schutzgruppen finden Sie unter [AWS Shield Advanced Schutzgruppen](#).

Wie AWS Shield mindert man Ereignisse

Die Abhilfelogik, die Ihre Anwendung schützt, kann je nach Anwendungsarchitektur variieren. Wenn Sie eine Webanwendung mit Amazon CloudFront und Amazon Route 53 schützen, profitieren Sie von Schutzmaßnahmen, die speziell auf Web- und DNS-Anwendungsfälle zugeschnitten sind und den gesamten Datenverkehr für die Services schützen. Wenn der Einstiegspunkt Ihrer Anwendung eine Ressource ist, die in einer AWS Region ausgeführt wird, variiert die Abhilfelogik je nach Service, Ressourcentyp und Nutzung von. AWS Shield Advanced

AWS Systeme zur DDoS-Abwehr werden von Shield-Ingenieuren entwickelt und sind eng in die Dienste integriert AWS . Die Techniker berücksichtigen Aspekte Ihrer Architektur wie die Kapazität und den Zustand der Zielressourcen. Die Techniker von Shield überwachen kontinuierlich die Wirksamkeit und Leistung von DDoS-Abwehrsystemen und sind in der Lage, schnell zu reagieren, wenn neue Bedrohungen entdeckt oder erwartet werden.

Sie können Ihre Anwendung so gestalten, dass sie bei erhöhtem Traffic oder hoher Auslastung skaliert wird, um sicherzustellen, dass sie nicht durch kleinere Anforderungsfluten beeinträchtigt wird. Wenn Sie Shield Advanced zum Schutz Ihrer Ressourcen verwenden, sind Sie gegen unerwartete Erhöhungen Ihrer Cloud-Rechnung abgesichert, die als Folge eines DDoS-Angriffs auftreten könnten.

Maßnahmen zur Minderung der Infrastruktur

Bei Angriffen auf Infrastrukturebene sind Systeme zur AWS Shield DDoS-Abwehr an der AWS Netzwerkgrenze und an Edge-Standorten AWS vorhanden. Die Platzierung mehrerer Ebenen von Sicherheitskontrollen in der gesamten AWS Infrastruktur sorgt für defense-in-depth Ihre Cloud-Anwendungen.

Shield unterhält Systeme zur DDoS-Abwehr an allen Zugangspunkten aus dem Internet. Wenn Shield einen DDoS-Angriff erkennt, leitet es den Datenverkehr für jeden Eingangspunkt durch die DDoS-Abwehrsysteme am selben Standort um. Dies führt zu keiner beobachtbaren zusätzlichen Latenz und bietet eine Abwehrkapazität von mehr als 100 TeraBits pro Sekunde (Tbps) in allen Regionen und allen Edge-Standorten. AWS Shield schützt Ihre Ressourcenverfügbarkeit, ohne den Datenverkehr an externe oder entfernte Scrubbing-Center umzuleiten, was die Latenz erhöhen könnte.

- An der AWS Netzwerkgrenze verhindern DDoS-Abwehrsysteme für jeden AWS Dienst oder jede Ressource Angriffe auf Infrastrukturebene, die aus dem Internet kommen. Die Systeme führen ihre Abhilfemaßnahmen durch, wenn sie von Shield Detection oder von einem Techniker des Shield Response Teams (SRT) gemeldet werden.
- An AWS Edge-Standorten überprüfen DDoS-Abwehrsysteme kontinuierlich jedes Paket, das an CloudFront Amazon-Distributionen und Amazon Route 53-Hosting-Zonen weitergeleitet wird, unabhängig von ihrer Herkunft. Bei Bedarf wenden die Systeme Schutzmaßnahmen an, die speziell für den Web- und DNS-Verkehr entwickelt wurden. Ein zusätzlicher Vorteil der Verwendung von Amazon CloudFront und Amazon Route 53 zum Schutz Ihrer Webanwendungen besteht darin, dass DDoS-Angriffe sofort abgewehrt werden, ohne dass ein Signal von der Shield-Erkennung erforderlich ist.

Abwehr auf Anwendungsebene

Shield Advanced bietet Schutzmaßnahmen auf Webanwendungsebene für die CloudFront Amazon-Distributionen und Application Load Balancer, für die Sie den erweiterten Schutz von Shield aktiviert haben. Wenn Sie den Schutz aktivieren, ordnen Sie der Ressource eine AWS WAF Web-ACL zu, um die Erkennung auf Webanwendungsebene zu aktivieren. Darüber hinaus haben Sie die Möglichkeit, die automatische Abwehr auf Anwendungsebene zu aktivieren, wodurch Shield Advanced angewiesen wird, den Schutz während eines DDoS-Angriffs für Sie zu verwalten.

Shield bietet nur benutzerdefinierte Abwehrmaßnahmen für Angriffe auf Anwendungsebene auf Ressourcen, für die Sie Shield Advanced aktiviert haben, und automatische Abwehr auf Anwendungsebene. Mit automatischer Abwehr erzwingt Shield Advanced eine AWS WAF Ratenbegrenzung für Anfragen von bekannten DDoS-Quellen und fügt als Reaktion auf erkannte DDoS-Angriffe automatisch benutzerdefinierte AWS WAF Schutzmaßnahmen hinzu und verwaltet diese. Ausführliche Informationen zu Abhilfemaßnahmen dieser Art finden Sie unter [So verwaltet Shield Advanced die automatische Schadensbegrenzung](#)

Eine ratenbasierte Regel in Ihrer Web-ACL, unabhängig davon, ob sie von Ihnen oder durch die automatische Abwehr auf Anwendungsebene von Shield Advanced hinzugefügt wurde, kann einen Angriff abwehren, bevor er ein erkennbares Ausmaß erreicht. Weitere Informationen zur Erkennung finden Sie unter [Erkennungslogik für Bedrohungen auf Anwendungsebene](#)

Funktionen zur Schadensbegrenzung

Die Hauptmerkmale der AWS Shield DDoS-Abwehr sind die folgenden:

- **Paketvalidierung** — Dadurch wird sichergestellt, dass jedes geprüfte Paket einer erwarteten Struktur entspricht und für sein Protokoll gültig ist. Zu den unterstützten Protokollvalidierungen gehören IP, TCP (einschließlich Header und Optionen), UDP, ICMP, DNS und NTP.
- **Zugriffskontrolllisten (ACLs) und Shaper** — Eine ACL bewertet den Datenverkehr anhand bestimmter Attribute und verwirft den entsprechenden Datenverkehr entweder oder ordnet ihn einem Shaper zu. Der Shaper begrenzt die Paketrage für den entsprechenden Datenverkehr und verwirft überschüssige Pakete, um das Volumen einzudämmen, das das Ziel erreicht. AWS Shield Die Techniker des Detection and Shield Response Teams (SRT) können spezielle Ratenzuweisungen für den erwarteten Verkehr und restriktivere Ratenzuweisungen für den Datenverkehr mit Attributen bereitstellen, die bekannten DDoS-Angriffsvektoren entsprechen. Zu den Attributen, denen eine ACL entsprechen kann, gehören der Port, das Protokoll, die TCP-Flags, die Zieladresse, das Quellland und beliebige Muster in der Paketnutzlast.
- **Bewertung von Verdachtsfällen** — Dabei wird das Wissen, das Shield über den erwarteten Datenverkehr hat, genutzt, um jedem Paket eine Bewertung zuzuweisen. Paketen, die sich eher an

Muster für zweifelsfrei funktionierenden Verkehr halten, wird eine niedrigere Verdachtsbewertung zugewiesen. Die Beobachtung von bekannten schlechten Datenverkehrsattributen kann die Verdachtsquote für ein Paket erhöhen. Wenn es notwendig ist, Pakete mit einer Ratenbegrenzung zu begrenzen, verwirft Shield zuerst Pakete mit höheren Verdachtswerten. Auf diese Weise kann Shield sowohl bekannte als auch Zero-Day-DDoS-Angriffe abwehren und gleichzeitig Fehlalarme vermeiden.

- **TCP-SYN-Proxy** — Dieser bietet Schutz vor TCP-SYN-Floods, indem TCP-SYN-Cookies gesendet werden, um neue Verbindungen herauszufordern, bevor sie an den geschützten Dienst weitergeleitet werden. Der von Shield DDoS Mitigation bereitgestellte TCP-SYN-Proxy ist zustandslos, sodass er die größten bekannten TCP-SYN-Flood-Angriffe abwehren kann, ohne die State-Erschöpfung zu erreichen. Dies wird erreicht, indem AWS Dienste integriert werden, um den Verbindungsstatus zu übergeben, anstatt einen kontinuierlichen Proxy zwischen dem Client und dem geschützten Dienst aufrechtzuerhalten. Der TCP-SYN-Proxy ist derzeit auf Amazon CloudFront und Amazon Route 53 verfügbar.
- **Ratenverteilung** — Dadurch werden die Shaper-Werte pro Standort kontinuierlich an das Eingangsmuster des Datenverkehrs zu einer geschützten Ressource angepasst. Dadurch wird verhindert, dass der Kundendatenverkehr, der möglicherweise nicht gleichmäßig in das Netzwerk gelangt, begrenzt wird. AWS

AWS Shield Mitigationslogik für CloudFront und Route 53

Shield DDoS Mitigation überprüft kontinuierlich den Verkehr für CloudFront und Route 53. Diese Dienste werden von einem weltweit verteilten Netzwerk von AWS Edge-Standorten aus betrieben, die Ihnen umfassenden Zugriff auf die DDoS-Abwehrkapazitäten von Shield bieten und Ihre Anwendung von einer Infrastruktur aus bereitstellen, die sich näher an Ihren Endbenutzern befindet.

- **CloudFront**— Durch Shield-DDoS-Abwehr kann nur Datenverkehr, der für Webanwendungen gültig ist, zum Service weitergeleitet werden. Dies bietet automatischen Schutz vor vielen gängigen DDoS-Vektoren wie UDP-Reflection-Angriffen.

CloudFront unterhält persistente Verbindungen zu Ihrem Anwendungsursprung, TCP-SYN-Floods werden durch die Integration mit der Shield-TCP-SYN-Proxyfunktion automatisch abgemildert und Transport Layer Security (TLS) wird am Edge beendet. Diese kombinierten Funktionen stellen sicher, dass Ihr Anwendungsursprung nur wohlgeformte Webanfragen empfängt und dass er vor DDoS-Angriffen auf niedrigerer Ebene, Verbindungsfluten und TLS-Missbrauch geschützt ist.

CloudFront verwendet eine Kombination aus DNS-Verkehrsrichtung und Anycast-Routing. Diese Techniken verbessern die Widerstandsfähigkeit Ihrer Anwendung, indem sie Angriffe direkt an der Quelle abwehren, Fehler isolieren und den Zugriff auf Kapazitäten sicherstellen, um die größten bekannten Angriffe abzuwehren.

- Route 53 — Shield-Schutzmaßnahmen ermöglichen es nur gültigen DNS-Anfragen, den Dienst zu erreichen. Shield verhindert DNS-Abfragefluten mithilfe einer Verdachtsbewertung, bei der bekanntermaßen funktionierende Abfragen priorisiert und Abfragen, die verdächtige oder bekannte DDoS-Angriffsattribute enthalten, depriorisiert werden.

Route 53 verwendet Shuffle-Sharding, um jeder gehosteten Zone einen eindeutigen Satz von vier Resolver-IP-Adressen bereitzustellen, sowohl für IPv4 als auch für IPv6. Jede IP-Adresse entspricht einer anderen Teilmenge von Route 53-Standorten. Jede Standortuntergruppe besteht aus autorisierenden DNS-Servern, die sich nur teilweise mit der Infrastruktur einer anderen Teilmenge überschneiden. Dadurch wird sichergestellt, dass eine Benutzerabfrage, falls sie aus irgendeinem Grund fehlschlägt, bei einem erneuten Versuch erfolgreich bearbeitet wird.

Route 53 verwendet Anycast-Routing, um DNS-Abfragen je nach Netzwerknähe an den nächstgelegenen Edge-Standort weiterzuleiten. Anycast fächert außerdem den DDoS-Verkehr zu vielen Edge-Standorten auf, wodurch verhindert wird, dass sich Angriffe auf einen einzigen Standort konzentrieren.

Zusätzlich zur Geschwindigkeit der Schadensbegrenzung bieten Route 53 einen breiten Zugang zu den weltweit verteilten Kapazitäten von Shield. CloudFront Um diese Funktionen zu nutzen, nutzen Sie diese Dienste als Einstiegspunkt für Ihre dynamischen oder statischen Webanwendungen.

Weitere Informationen zur Verwendung von CloudFront und Route 53 zum Schutz von Webanwendungen finden Sie unter [So schützen Sie dynamische Webanwendungen vor DDoS-Angriffen mithilfe von Amazon CloudFront und Amazon Route 53](#). Weitere Informationen zur Fehlerisolierung auf Route 53 finden Sie unter [Eine Fallstudie zur globalen Fehlerisolierung](#).

AWS Shield Minderungslogik für Regionen AWS

Ressourcen, die in AWS Regionen gestartet werden, werden durch AWS Shield DDoS-Abwehrsysteme geschützt, die von Shield auf Ressourcenebene erkannt werden. Zu den regionalen Ressourcen gehören Elastic IPs (EIPs), Classic Load Balancers und Application Load Balancers.

Vor der Einführung einer Risikominderung identifiziert Shield die Zielressource und ihre Kapazität. Shield verwendet die Kapazität, um den maximalen Gesamtverkehr zu bestimmen, den seine

Abhilfemaßnahmen für die Weiterleitung an die Ressource zulassen sollten. Zugriffskontrolllisten (ACLs) und andere Shaper im Rahmen der Abwehr können das zulässige Volumen für bestimmten Datenverkehr verringern, z. B. für Datenverkehr, der bekannten DDoS-Angriffsvektoren entspricht oder von dem nicht erwartet wird, dass er in großem Umfang übertragen wird. Dadurch wird der Umfang des Datenverkehrs, den die Abhilfemaßnahmen für UDP-Reflection-Angriffe oder für TCP-Verkehr mit TCP-SYN- oder FIN-Flags zulassen, weiter begrenzt.

Shield bestimmt die Kapazität und platziert die Abhilfemaßnahmen für jeden Ressourcentyp unterschiedlich.

- Für eine Amazon EC2 EC2-Instance oder eine EIP, die an eine Amazon EC2 EC2-Instance angehängt ist, berechnet Shield die Kapazität auf der Grundlage des Instance-Typs und anderer Instance-Attribute, z. B. ob für die Instance Enhanced Networking aktiviert ist.
- Für einen Application Load Balancer oder Classic Load Balancer berechnet Shield die Kapazität individuell für jeden Zielknoten des Load Balancers. Die Abwehr von DDoS-Angriffen für diese Ressourcen erfolgt durch eine Kombination aus Shield DDoS-Abwehr und automatischer Skalierung durch den Load Balancer. Wenn das Shield Response Team (SRT) an einem Angriff gegen eine Application Load Balancer- oder Classic Load Balancer Balancer-Ressource beteiligt ist, kann es die Skalierung als zusätzliche Schutzmaßnahme beschleunigen.
- Shield berechnet die Kapazität für einige AWS Ressourcen auf der Grundlage der verfügbaren Kapazität der zugrunde liegenden AWS Infrastruktur. Zu diesen Ressourcentypen gehören Network Load Balancer (NLBs) und Ressourcen, die den Verkehr über Gateway Load Balancer weiterleiten oder. AWS Network Firewall

Note

Schützen Sie Ihre Network Load Balancer, indem Sie EIPs anhängen, die durch Shield Advanced geschützt sind. Sie können mit SRT zusammenarbeiten, um benutzerdefinierte Abhilfemaßnahmen zu erstellen, die auf dem erwarteten Datenverkehr und der Kapazität der zugrunde liegenden Anwendung basieren.

Wenn Shield eine Abwehr einführt, werden die anfänglichen Ratenbegrenzungen, die Shield in der Abwehrlogik definiert, gleichermaßen auf jedes Shield-DDoS-Abwehrsystem angewendet. Wenn Shield beispielsweise eine Risikominderung mit einem Limit von 100.000 Paketen pro Sekunde (pps) festlegt, werden zunächst 100.000 pps an jedem Standort zugelassen. Anschließend aggregiert Shield kontinuierlich Messwerte zur Risikominderung, um den tatsächlichen Verkehrsanteil zu

ermitteln, und verwendet dieses Verhältnis, um das Ratenlimit für jeden Standort anzupassen. Dadurch werden Fehlalarme verhindert und sichergestellt, dass die Maßnahmen nicht zu großzügig sind.

AWS Shield Risikominderungslogik für AWS Global Accelerator Standardbeschleuniger

Durch Shield-Schutzmaßnahmen kann nur gültiger Datenverkehr die Listener-Endpunkte eines Global Accelerator-Standardbeschleunigers erreichen. Standardbeschleuniger werden weltweit eingesetzt und stellen Ihnen IP-Adressen zur Verfügung, mit denen Sie den Datenverkehr an AWS Ressourcen in jeder Region weiterleiten können. AWS Die Ratenbegrenzungen, die Shield für eine Global-Accelerator-Minderung durchsetzt, basieren auf den Kapazitäten der Ressourcen, zu denen der Standard-Accelerator den Verkehr weiterleitet. Shield setzt Abhilfemaßnahmen ein, wenn der Gesamtverkehr die festgelegte Rate überschreitet und auch, wenn ein Bruchteil dieser Rate bei bekannten DDoS-Vektoren überschritten wird.

Wenn Sie einen Standardbeschleuniger konfigurieren, definieren Sie Endpunktgruppen für jede AWS Region, in die Sie den Datenverkehr für Ihre Anwendung weiterleiten. Wenn Shield eine Abwehr einführt, berechnet es die Kapazität jeder Endpunktgruppe und aktualisiert die Ratenlimits für jedes Shield DDoS-Abwehrsystem entsprechend. Die Rate variiert je nach Standort und basiert auf Annahmen von Shield darüber, wie der Verkehr vom Internet zu Ihren AWS Ressourcen geleitet wird. Die Kapazität für eine Endpunktgruppe wird berechnet als die Anzahl der Ressourcen in der Gruppe multipliziert mit der niedrigsten Kapazität für jede Ressource in der Gruppe. In regelmäßigen Abständen berechnet Shield die Kapazität für Ihre Anwendung neu und aktualisiert die Ratenlimits nach Bedarf.

Note

Die Verwendung von Verkehrswahlnummern zur Änderung des Prozentsatzes des Datenverkehrs, der an eine Endpunktgruppe geleitet wird, ändert nichts daran, wie Shield die Ratenlimits berechnet oder an seine DDoS-Abwehrsysteme verteilt. Wenn Sie Traffic Dials verwenden, konfigurieren Sie Ihre Endpunktgruppen so, dass sie sich in Bezug auf Ressourcentyp und -menge gegenseitig spiegeln. Dadurch wird sichergestellt, dass die von Shield berechnete Kapazität repräsentativ für die Ressourcen ist, die den Datenverkehr für Ihre Anwendung bereitstellen.

Weitere Informationen zu Endpunktgruppen und Verkehrswahlen in Global Accelerator finden Sie unter [Endpunktgruppen in AWS Global Accelerator Standard-Beschleunigern](#).

AWS Shield Advanced Schadensbegrenzungslogik für Elastic IPs

Wenn Sie eine Elastic IP (EIP) mit schützen AWS Shield Advanced, verbessert Shield Advanced die Schutzmaßnahmen, die Shield während eines DDoS-Ereignisses einleitet. Shield Advanced DDoS-Abwehrsysteme replizieren die Network ACL (NACL) -Konfiguration für das öffentliche Subnetz, dem die EIP zugeordnet ist. Wenn Ihre NACL beispielsweise so konfiguriert ist, dass sie den gesamten UDP-Verkehr blockiert, führt Shield Advanced diese Regel mit den von Shield festgelegten Abhilfemaßnahmen zusammen.

Diese zusätzliche Funktionalität kann Ihnen helfen, Verfügbarkeitsrisiken aufgrund von Datenverkehr zu vermeiden, der für Ihre Anwendung nicht gültig ist. Sie können NACLs auch verwenden, um einzelne Quell-IP-Adressen oder CIDR-Bereiche für Quell-IP-Adressen zu blockieren. Dies kann ein nützliches Tool zur Abwehr von DDoS-Angriffen sein, die nicht verteilt werden. Außerdem können Sie damit ganz einfach Ihre eigenen Zulassungslisten verwalten oder IP-Adressen blockieren, die nicht mit Ihrer Anwendung kommunizieren sollen, ohne auf das Eingreifen von AWS Technikern angewiesen zu sein.

AWS Shield Advanced Schadensbegrenzungslogik für Webanwendungen

AWS Shield Advanced wird verwendet AWS WAF , um Angriffe auf Webanwendungsebene abzuwehren. AWS WAF ist in Shield Advanced ohne zusätzliche Kosten enthalten.

Standardschutz auf Anwendungsebene

Wenn Sie eine CloudFront Amazon-Distribution oder einen Application Load Balancer mit Shield Advanced schützen, können Sie Shield Advanced verwenden, um Ihrer geschützten Ressource eine AWS WAF Web-ACL zuzuordnen, sofern Ihnen noch keine zugeordnet ist. Wenn Sie noch keine Web-ACL konfiguriert haben, können Sie mit dem Shield Advanced-Konsolenassistenten eine erstellen und ihr eine ratenbasierte Regel hinzufügen. Eine ratenbasierte Regel begrenzt die Anzahl der Anfragen pro Fünf-Minuten-Zeitfenster für jede IP-Adresse und bietet so grundlegenden Schutz vor einer Flut von Anfragen auf Webanwendungsebene. Sie können die Rate so konfigurieren, dass sie bei 100 beginnt. Weitere Informationen finden Sie unter [Shield Advanced AWS WAF Web-ACLs und ratenbasierte Regeln auf Anwendungsebene](#).

Sie können den AWS WAF Dienst auch zur Verwaltung der Web-ACL verwenden. Auf diese Weise können Sie die Web-ACL-Konfiguration erweitern AWS WAF, um beispielsweise

bestimmte Webanforderungskomponenten auf Übereinstimmungen oder Muster zu überprüfen, benutzerdefinierte Anfragen- und Antwortbehandlungen hinzuzufügen und Abgleiche mit der Geolokalisierung des Absenders der Anfrage durchzuführen. Weitere Informationen zu AWS WAF Regeln finden Sie unter [AWS WAF Regeln](#)

Automatische Schadensbegrenzung auf Anwendungsebene

Um den Schutz zu verbessern, aktivieren Sie die automatische Abwehr auf Anwendungsebene mit Shield Advanced. Mit dieser Option behält Shield Advanced eine Regel zur AWS WAF Geschwindigkeitsbegrenzung für Anfragen von bekannten DDoS-Quellen bei und bietet benutzerdefinierte Abhilfemaßnahmen für erkannte DDoS-Angriffe.

Wenn Shield Advanced einen Angriff auf eine geschützte Ressource erkennt, versucht es, eine Angriffssignatur zu identifizieren, die den Angriffsverkehr vom normalen Verkehr zu Ihrer Anwendung isoliert. Shield Advanced bewertet die identifizierte Angriffssignatur anhand der historischen Verkehrsmuster für die angegriffene Ressource sowie für jede andere Ressource, die derselben Web-ACL zugeordnet ist.

Wenn Shield Advanced feststellt, dass die Angriffssignatur nur den Datenverkehr isoliert, der an dem DDoS-Angriff beteiligt ist, implementiert es die Signatur in AWS WAF Regeln innerhalb der zugehörigen Web-ACL. Sie können Shield Advanced anweisen, Abhilfemaßnahmen zu platzieren, die nur den Datenverkehr zählen, mit dem sie übereinstimmen, oder ihn blockieren, und Sie können die Einstellung jederzeit ändern. Wenn Shield Advanced feststellt, dass seine Schadensbegrenzungsregeln nicht mehr benötigt werden, werden sie aus der Web-ACL entfernt. Weitere Informationen zur Abwehr von Ereignissen auf Anwendungsebene finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#)

Weitere Informationen zu Schutzmaßnahmen auf Anwendungsebene von Shield Advanced finden Sie unter [AWS Shield Advanced Schutzmaßnahmen auf Anwendungsebene \(Schicht 7\)](#).

Beispiele für grundlegende DDoS-resistente Architekturen

DDoS-Resilienz ist die Fähigkeit Ihrer Anwendungsarchitektur, Distributed-Denial-of-Service-Angriffen (DDoS) standzuhalten und gleichzeitig legitime Endbenutzer zu bedienen. Eine Anwendung, die sehr widerstandsfähig ist, kann während eines Angriffs verfügbar bleiben, ohne dass sich dies auf Leistungskennzahlen wie Fehler oder Latenz auswirkt. Dieser Abschnitt zeigt einige gängige Beispielsarchitekturen und beschreibt, wie die von Shield Advanced bereitgestellten Funktionen zur DDoS-Erkennung und -Abwehr verwendet werden können, um AWS ihre DDoS-Resilienz zu erhöhen.

In den Beispielarchitekturen in diesem Abschnitt werden die AWS Dienste hervorgehoben, die die größten Vorteile bei der DDoS-Resilienz für Ihre bereitgestellten Anwendungen bieten. Zu den Vorteilen der hervorgehobenen Dienste gehören die folgenden:

- Zugriff auf weltweit verteilte Netzwerkkapazitäten — Die Dienste Amazon CloudFront und Amazon Route 53 bieten Ihnen Zugriff auf Internet- und DDoS-Abwehrkapazitäten im gesamten AWS globalen Edge-Netzwerk. AWS Global Accelerator Dies ist nützlich, um größere volumetrische Angriffe abzuwehren, die eine Größenordnung von Terabit erreichen können. Sie können Ihre Anwendung in jeder AWS Region ausführen und diese Dienste nutzen, um die Verfügbarkeit zu schützen und die Leistung für Ihre legitimen Benutzer zu optimieren.
- Schutz vor DDoS-Angriffsvektoren auf Webanwendungsebene — DDoS-Angriffe auf Webanwendungsebene lassen sich am besten mit einer Kombination aus Anwendungsskala und einer Web Application Firewall (WAF) abwehren. Shield Advanced verwendet Protokolle zur Inspektion von Webanfragen AWS WAF, um Anomalien zu erkennen, die entweder automatisch oder durch Zusammenarbeit mit dem AWS Shield Response Team (SRT) behoben werden können. Automatische Abwehr ist durch bereitgestellte AWS WAF ratenbasierte Regeln und auch durch die automatische DDoS-Abwehr auf Anwendungsebene von Shield Advanced verfügbar.

[Lesen Sie sich nicht nur diese Beispiele durch, sondern überprüfen Sie auch die geltenden Best Practices unter AWS Best Practices for DDoS Resiliency und befolgen Sie diese.](#)

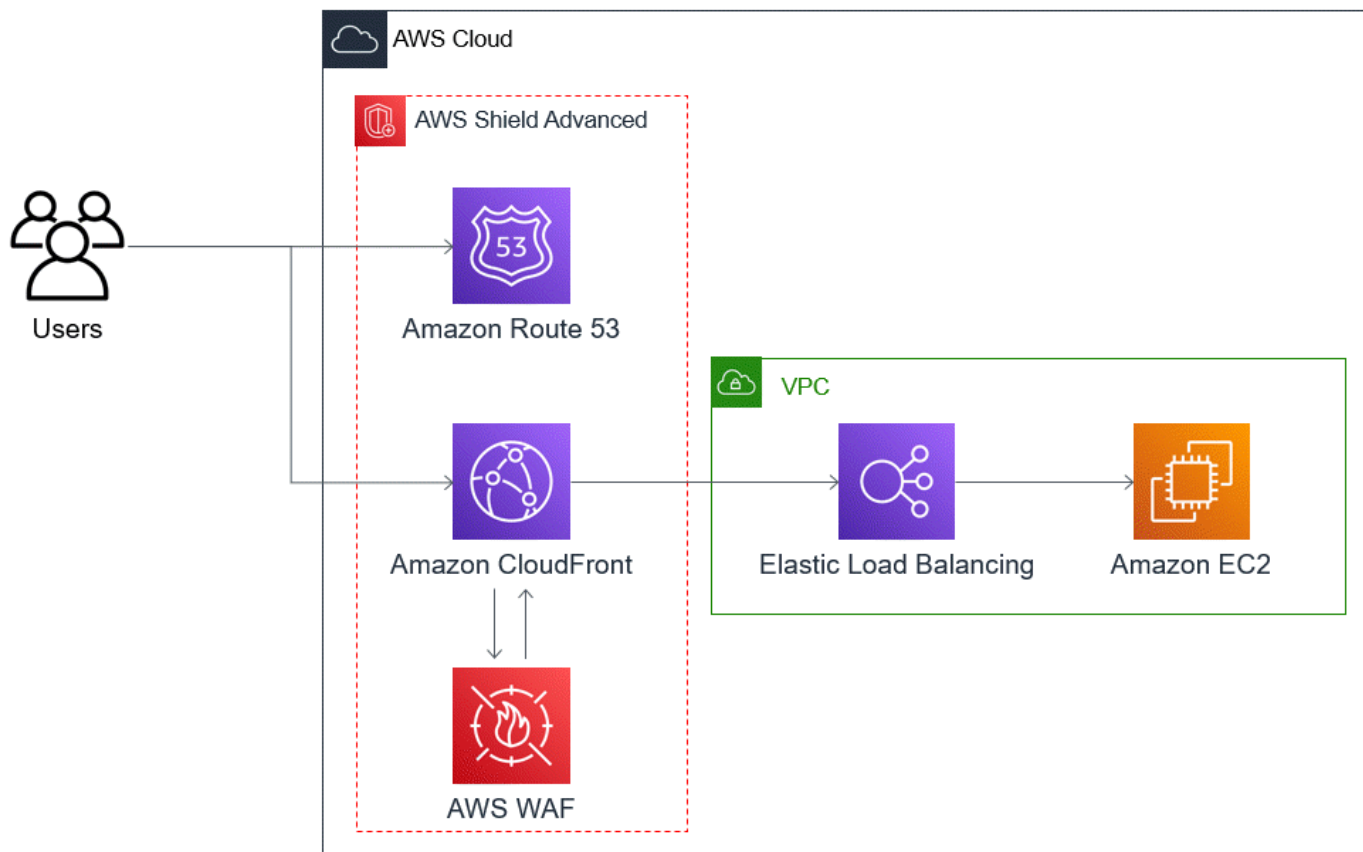
Beispiel für DDoS-Resilienz für gängige Webanwendungen

Sie können eine Webanwendung in jeder AWS Region erstellen und automatischen DDoS-Schutz durch die Erkennungs- und Abwehrfunktionen in der Region erhalten. AWS

Dieses Beispiel bezieht sich auf Architekturen, die Benutzer mithilfe von Ressourcen wie Classic Load Balancern, Application Load Balancern, Network Load Balancern, AWS Marketplace-Lösungen oder Ihrer eigenen Proxyschicht zu einer Webanwendung weiterleiten. Sie können die DDoS-Resilienz verbessern, indem Sie Amazon Route 53-Hosting-Zonen, CloudFront Amazon-Distributionen und AWS WAF Web-ACLs zwischen diesen Webanwendungsressourcen und Ihren Benutzern einfügen. Diese Einfügungen können den Ursprung der Anwendung verschleiern, Anfragen näher an Ihren Endbenutzern bearbeiten und eine Flut von Anfragen auf Anwendungsebene erkennen und verhindern. Anwendungen, die Ihren Benutzern statische oder dynamische Inhalte mit CloudFront und Route 53 bereitstellen, sind durch ein integriertes, vollständig integriertes DDoS-Abwehrsystem geschützt, das Angriffe auf Infrastrukturebene in Echtzeit abwehrt.

Mit diesen architektonischen Verbesserungen können Sie dann Ihre von Route 53 gehosteten Zonen und Ihre CloudFront Distributionen mit Shield Advanced schützen. Wenn Sie CloudFront Distributionen schützen, fordert Shield Advanced Sie auf, AWS WAF Web-ACLs zuzuordnen und ratenbasierte Regeln für diese zu erstellen. Außerdem haben Sie die Möglichkeit, automatische DDoS-Abwehr auf Anwendungsebene oder proaktives Engagement zu aktivieren. Proaktives Engagement und automatische DDoS-Abwehr auf Anwendungsebene verwenden Route 53-Zustandsprüfungen, die Sie der Ressource zuordnen. Weitere Informationen zu diesen Optionen finden Sie unter [Ressourcenschutz in AWS Shield Advanced](#).

Das folgende Referenzdiagramm zeigt diese DDoS-resistente Architektur für eine Webanwendung.



Zu den Vorteilen, die dieser Ansatz für Ihre Webanwendung bietet, gehören die folgenden:

- Schutz vor häufig genutzten DDoS-Angriffen auf Infrastrukturebene (Layer 3 und Layer 4) ohne Erkennungsverzögerung. Wenn eine Ressource häufig angegriffen wird, führt Shield Advanced außerdem Schutzmaßnahmen für längere Zeiträume durch. Shield Advanced verwendet auch den Anwendungskontext, der von Netzwerk-ACLs (NACLs) abgeleitet wird, um unerwünschten

Datenverkehr weiter flussaufwärts zu blockieren. Dadurch werden Fehler isoliert, die näher an ihrer Quelle liegen, wodurch die Auswirkungen auf legitime Benutzer minimiert werden.

- Schutz vor TCP-SYN-Floods. Die in Route 53 integrierten Systeme zur DDoS-Abwehr AWS Global Accelerator bieten eine TCP-SYN-Proxyfunktion, die neue Verbindungsversuche abwehrt und nur legitimen Benutzern dient. CloudFront
- Schutz vor Angriffen auf DNS-Anwendungsebene, da Route 53 für die Bereitstellung autorisierender DNS-Antworten verantwortlich ist.
- Schutz vor Fluten von Anfragen auf der Webanwendungsebene. Die ratenbasierte Regel, die Sie in Ihrer AWS WAF Web-ACL konfigurieren, blockiert Quell-IPs, wenn sie mehr Anfragen senden, als die Regel zulässt.
- Automatische DDoS-Abwehr auf Anwendungsebene für Ihre CloudFront Distributionen, wenn Sie diese Option aktivieren. Bei der automatischen DDoS-Abwehr behält Shield Advanced eine ratenbasierte Regel in der zugehörigen AWS WAF Web-ACL der Distribution bei, die das Volumen der Anfragen von bekannten DDoS-Quellen begrenzt. Wenn Shield Advanced ein Ereignis erkennt, das sich auf den Zustand Ihrer Anwendung auswirkt, erstellt, testet und verwaltet es außerdem automatisch Abhilferegeln in der Web-ACL.
- Proaktive Zusammenarbeit mit dem Shield Response Team (SRT), wenn Sie diese Option aktivieren. Wenn Shield Advanced ein Ereignis erkennt, das sich auf den Zustand Ihrer Anwendung auswirkt, reagiert das SRT und setzt sich anhand der von Ihnen angegebenen Kontaktinformationen proaktiv mit Ihren Sicherheits- oder Betriebsteams in Verbindung. Das SRT analysiert Muster in Ihrem Datenverkehr und kann Ihre AWS WAF Regeln aktualisieren, um den Angriff zu blockieren.

Beispiel für DDoS-Resilienz für TCP- und UDP-Anwendungen

Dieses Beispiel zeigt eine DDoS-resistente Architektur für TCP- und UDP-Anwendungen in einer AWS Region, die Amazon Elastic Compute Cloud (Amazon EC2) -Instances oder Elastic IP (EIP) -Adressen verwendet.

Sie können diesem allgemeinen Beispiel folgen, um die DDoS-Resilienz für die folgenden Anwendungstypen zu verbessern:

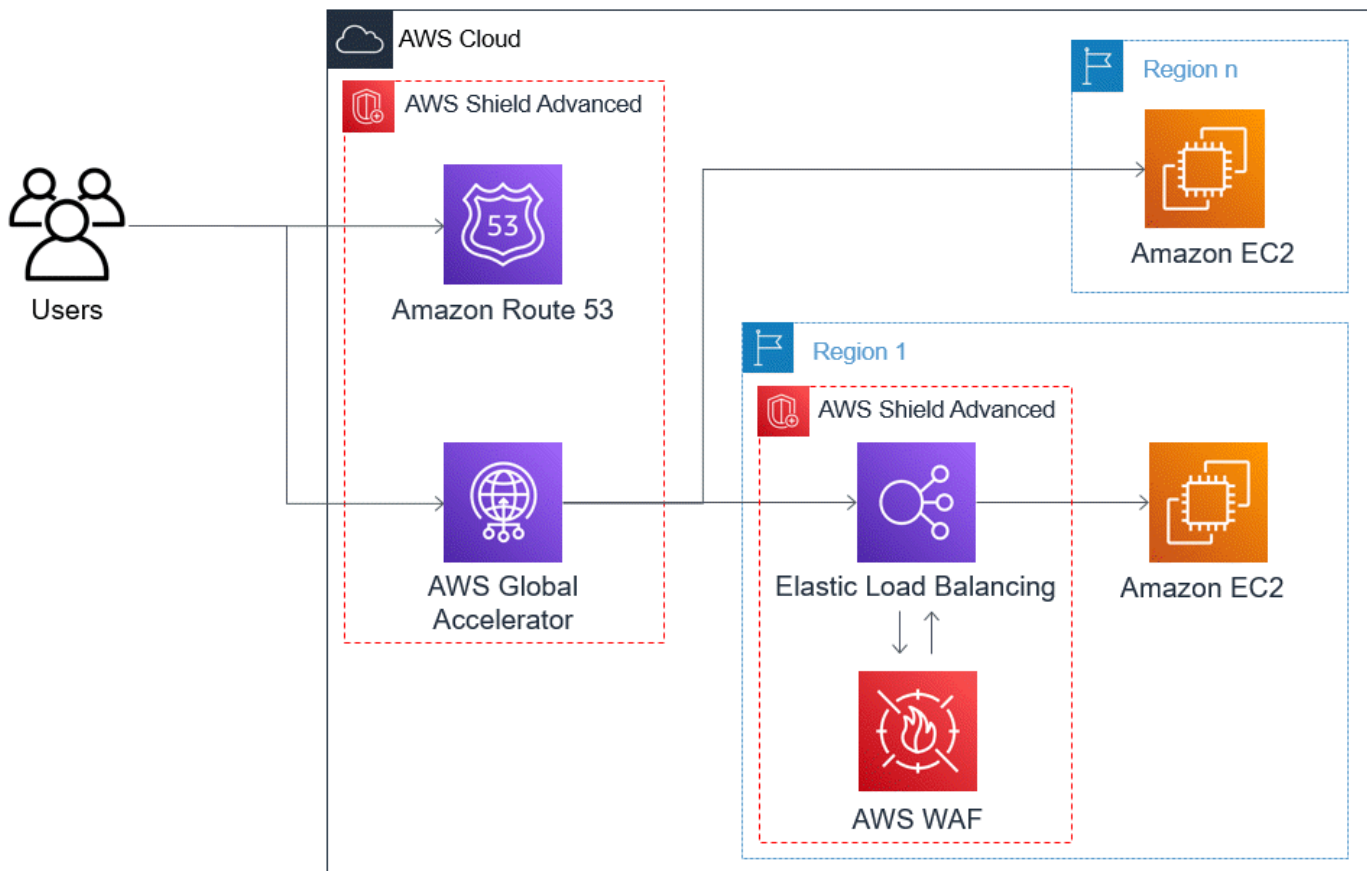
- TCP- oder UDP-Anwendungen. Zum Beispiel Anwendungen, die für Spiele, IoT und Voice over IP verwendet werden.
- Webanwendungen, die statische IP-Adressen benötigen oder Protokolle verwenden, die Amazon CloudFront nicht unterstützt. Beispielsweise benötigt Ihre Anwendung möglicherweise IP-Adressen,

die Ihre Benutzer zu ihren Firewall-Zulassungslisten hinzufügen können und die nicht von anderen AWS Kunden verwendet werden.

Sie können die DDoS-Resilienz für diese Anwendungstypen verbessern, indem Sie Amazon Route 53 und einführen. AWS Global Accelerator Diese Dienste können Benutzer zu Ihrer Anwendung weiterleiten und sie können Ihrer Anwendung statische IP-Adressen zur Verfügung stellen, die per Anycast über das AWS globale Edge-Netzwerk weitergeleitet werden. Die Standardbeschleuniger von Global Accelerator können die Benutzerlatenz um bis zu 60% verbessern. Wenn Sie über eine Webanwendung verfügen, können Sie Anforderungsfluten auf der Webanwendungsebene erkennen und verhindern, indem Sie die Anwendung auf einem Application Load Balancer ausführen und den Application Load Balancer anschließend mit einer AWS WAF Web-ACL schützen.

Nachdem Sie Ihre Anwendung erstellt haben, schützen Sie Ihre Route 53-Hosting-Zonen, Global Accelerator-Standardbeschleuniger und alle Application Load Balancer mit Shield Advanced. Wenn Sie Ihre Application Load Balancers schützen, können Sie AWS WAF Web-ACLs verknüpfen und ratenbasierte Regeln für sie erstellen. Sie können die proaktive Zusammenarbeit mit dem SRT sowohl für Ihre Global Accelerator-Standardbeschleuniger als auch für Ihre Application Load Balancer konfigurieren, indem Sie neue oder bestehende Route 53-Zustandsprüfungen zuordnen. Weitere Informationen zu den Optionen finden Sie unter. [Ressourcenschutz in AWS Shield Advanced](#)

Das folgende Referenzdiagramm zeigt ein Beispiel für eine DDoS-resistente Architektur für TCP- und UDP-Anwendungen.



Zu den Vorteilen, die dieser Ansatz für Ihre Anwendung bietet, gehören die folgenden:

- Schutz vor den größten bekannten DDoS-Angriffen auf Infrastrukturebene (Layer 3 und Layer 4). Wenn das Volumen eines Angriffs zu einer Überlastung im Vorfeld führt, wird der Fehler näher an seiner Quelle isoliert und hat nur minimale Auswirkungen auf Ihre legitimen Benutzer.
- Schutz vor Angriffen auf DNS-Anwendungsebene, da Route 53 für die Bereitstellung autorisierender DNS-Antworten verantwortlich ist.
- Wenn Sie über eine Webanwendung verfügen, bietet dieser Ansatz Schutz vor einer Flut von Anfragen auf der Webanwendungsebene. Die ratenbasierte Regel, die Sie in Ihrer AWS WAF Web-ACL konfigurieren, blockiert Quell-IPs, obwohl diese mehr Anfragen senden, als die Regel zulässt.
- Proaktive Zusammenarbeit mit dem Shield Response Team (SRT), wenn Sie diese Option für berechnete Ressourcen aktivieren möchten. Wenn Shield Advanced ein Ereignis erkennt, das sich auf den Zustand Ihrer Anwendung auswirkt, reagiert das SRT und setzt sich anhand der von Ihnen angegebenen Kontaktinformationen proaktiv mit Ihren Sicherheits- oder Betriebsteams in Verbindung.

Beispiele für Shield Advanced-Anwendungsfälle

Sie können Shield Advanced verwenden, um Ihre Ressourcen in vielen Szenarien zu schützen. In einigen Fällen sollten Sie jedoch andere Dienste verwenden oder andere Dienste mit Shield Advanced kombinieren, um den besten Schutz zu bieten. Im Folgenden finden Sie Beispiele dafür, wie Sie Shield Advanced oder andere AWS Dienste verwenden können, um Ihre Ressourcen zu schützen.

Ziel	Empfohlene Services	Zugehörige Servicedokumentation
Schutz einer Webanwendung und RESTful-APIs gegen einen DDoS-Angriff	Shield Advanced schützt eine CloudFront Amazon-Distribution und einen Application Load Balancer	Elastic Load Balancing Balancing-Dokumentation , CloudFront Amazon-Dokumentation
Schutz einer TCP-basierten Anwendung gegen einen DDoS-Angriff	Shield Advanced schützt einen AWS Global Accelerator Standardbeschleuniger, der an eine Elastic IP-Adresse angeschlossen ist	AWS Global Accelerator Dokumentation , Elastic Load Balancing Balancing-Dokumentation
Schutz eines auf UDP basierenden Game-Servers gegen einen DDoS-Angriff	Shield Advanced schützt eine Amazon EC2 EC2-Instance, die an eine Elastic IP-Adresse angeschlossen ist	Amazon Elastic Compute Cloud-Dokumentation

Wenn Sie beispielsweise Shield Advanced verwenden, um eine Elastic IP-Adresse zu schützen, schützt Shield Advanced die damit verbundene Ressource. Während eines Angriffs verteilt Shield Advanced Ihre Netzwerk-ACLs automatisch an der Netzwerkgrenze. Wenn sich Ihre Netzwerk-ACLs an der Netzwerkgrenze befinden, kann Shield Advanced Schutz vor größeren DDoS-Ereignissen bieten. In der Regel werden Netzwerk-ACLs in der Nähe Ihrer Amazon EC2 EC2-Instances innerhalb Ihrer Amazon VPC angewendet. Die Netzwerk-ACL kann Angriffe nur so groß abwehren, wie Ihre Amazon VPC und Instance bewältigen können. Wenn die an Ihre Amazon EC2 EC2-Instance angeschlossene Netzwerkschnittstelle bis zu 10 Gbit/s verarbeiten kann, werden Volumes über 10 Gbit/s langsamer und blockieren möglicherweise den Datenverkehr zu dieser Instance. Während eines Angriffs befördert Shield Advanced Ihre Netzwerk-ACL bis AWS an die

Grenze, wodurch mehrere Terabyte an Datenverkehr verarbeitet werden können. Ihre Netzwerk-ACL kann Schutz für Ihre Ressource weit über die typische Kapazität Ihres Netzwerks hinaus bieten. Weitere Informationen zu Netzwerk-ACLs finden Sie unter [Network ACLs](#).

Erste Schritte mit AWS Shield Advanced

Dieses Tutorial führt Sie durch die ersten Schritte mit der AWS Shield Advanced Verwendung der Shield Advanced-Konsole.

Note

Shield Advanced erfordert ein Abonnement, AWS Shield Standard aber nicht. Die von Shield Standard bereitgestellten Schutzmaßnahmen stehen allen AWS Kunden kostenlos zur Verfügung.

Shield Advanced bietet fortschrittlichen Schutz vor DDoS-Erkennung und -Abwehr für Angriffe auf Netzwerkschicht (Schicht 3), Transportschicht (Schicht 4) und Anwendungsebene (Schicht 7). Weitere Informationen zu Shield Advanced finden Sie unter [AWS Shield Advanced Überblick](#).

Die AWS technische Gemeinschaft hat Informationen über eine Beispieloption mit einem Klick für die Verwendung AWS CloudFormation und AWS Firewall Manager Konfiguration von Shield Advanced veröffentlicht. Sie können Firewall Manager verwenden, wenn Ihre Konten Teil einer Organisation in sind AWS Organizations und wenn Sie alle Ressourcentypen außer Amazon Route 53 oder schützen AWS Global Accelerator. Weitere Informationen zu dieser Option finden Sie im Tutorial unter [Bereitstellung von Shield Advanced mit einem Klick](#).

Note

Es ist wichtig, dass Sie Shield Advanced vor einem Distributed Denial of Service (DDoS) - Ereignis vollständig konfigurieren. Schließen Sie die Konfiguration ab, um sicherzustellen, dass Ihre Anwendung geschützt ist und dass Sie bereit sind, zu reagieren, falls Ihre Anwendung von einem DDoS-Angriff betroffen ist.

Führen Sie die folgenden Schritte der Reihe nach aus.

Inhalt

- [Abonnieren AWS Shield Advanced](#)
- [Ressourcen hinzufügen, um Schutzmaßnahmen zu schützen und zu konfigurieren](#)
 - [Konfigurieren Sie den DDoS-Schutz auf Anwendungsebene \(Schicht 7\) mit AWS WAF](#)
 - [Konfigurieren Sie die gesundheitsbasierte Erkennung für Ihren Schutz](#)
 - [Alarime und Benachrichtigungen konfigurieren](#)
 - [Überprüfen und beenden Sie Ihre Schutzkonfiguration](#)
- [AWS SRT-Unterstützung konfigurieren](#)
- [Erstellen Sie ein DDoS-Dashboard CloudWatch und stellen Sie Alarime ein CloudWatch](#)

Abonnieren AWS Shield Advanced

Sie müssen Shield Advanced für jeden abonnieren AWS-Konto, den Sie schützen möchten. Sie müssen Shield Standard nicht abonnieren.

Abrechnung des Shield Advanced-Abonnements

Wenn Sie ein AWS Channel-Wiederverkäufer sind, wenden Sie sich an Ihr Account-Team, um Informationen und Beratung zu erhalten. Diese Rechnungsinformationen gelten für Kunden, die keine AWS Channel-Wiederverkäufer sind.

Für alle anderen gelten die folgenden Abonnement- und Abrechnungsrichtlinien:

- Bei Konten, die Mitglieder einer AWS Organizations Organisation sind, werden die Shield Advanced-Abonnements mit dem Zahlerkonto der Organisation in AWS Rechnung gestellt, unabhängig davon, ob das Zahlerkonto selbst abonniert ist.
- Wenn Sie mehrere Konten abonnieren, die sich in derselben [Kontenfamilie mit AWS Organizations konsolidierter Abrechnung](#) befinden, deckt ein Abonnementpreis alle abonnierten Konten in der Familie ab. Die Organisation muss Eigentümer aller ihrer Ressourcen sein. AWS-Konten
- Wenn Sie mehrere Konten für mehrere Organisationen abonnieren, können Sie trotzdem eine Abonnementgebühr für alle Organisationen, Konten und Ressourcen zahlen, vorausgesetzt, Sie besitzen alle Konten. Wenden Sie sich an Ihren Kundenbetreuer oder AWS Support und beantragen Sie eine Gebührenbefreiung der AWS Shield Advanced Abonnementgebühren für alle Organisationen außer einer.

Detaillierte Preisinformationen und Beispiele finden Sie unter [AWS Shield Preisgestaltung](#).

Vereinfachen Sie Abonnements mit AWS Firewall Manager

Wenn Ihre Konten Teil einer Organisation sind, empfehlen wir Ihnen, diese Option zu verwenden AWS Firewall Manager , um Ihre Abonnements und Schutzmaßnahmen für die Organisation zu automatisieren. Firewall Manager unterstützt alle geschützten Ressourcentypen mit Ausnahme von Amazon Route 53 und AWS Global Accelerator. Informationen zur Verwendung von Firewall Manager finden Sie unter [AWS Firewall Manager](#) und [Erste Schritte mit AWS Firewall Manager](#) [AWS Shield Advanced Richtlinien](#).

Wenn Sie Firewall Manager nicht verwenden, abonnieren und fügen Sie für jedes Konto mit zu schützenden Ressourcen Schutzmaßnahmen hinzu. Gehen Sie dabei wie folgt vor.

Um ein Konto zu abonnieren AWS Shield Advanced

1. Melden Sie sich bei der AWS WAF & Shield-Konsole an AWS Management Console und öffnen Sie sie unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie in der AWS Shield Navigationsleiste Erste Schritte aus. Wählen Sie Shield Advanced abonnieren.
3. Lesen Sie auf der Seite Shield Advanced abonnieren die einzelnen Bestimmungen der Vereinbarung und aktivieren Sie dann alle Kontrollkästchen, um anzugeben, dass Sie die Bedingungen akzeptieren. Bei Konten in einer konsolidierten Fakturierungsfamilie müssen Sie den Bedingungen für jedes Konto zustimmen.

Important

Wenn Sie ein Abonnement abgeschlossen haben, müssen Sie sich an uns wenden [AWS Support](#), um das Abonnement zu kündigen.

[Um die automatische Verlängerung für Ihr Abonnement zu deaktivieren, müssen Sie den Shield-API-Vorgang UpdateSubscription oder den CLI-Befehl update-subscription verwenden.](#)

Wählen Sie Shield Advanced abonnieren. Dadurch abonniert Ihr Konto Shield Advanced und aktiviert den Dienst.

Ihr Konto ist abonniert. Führen Sie die folgenden Schritte aus, um die Ressourcen Ihres Kontos mit Shield Advanced zu schützen.

Note

Shield Advanced schützt Ihre Ressourcen nicht automatisch, nachdem Sie sich angemeldet haben. Sie müssen die Ressourcen angeben, die Shield Advanced schützen soll, und die Schutzmaßnahmen konfigurieren.

Ressourcen hinzufügen, um Schutzmaßnahmen zu schützen und zu konfigurieren

Shield Advanced schützt nur die Ressourcen, die Sie entweder über Shield Advanced oder in einer Firewall Manager Shield Advanced-Richtlinie angeben. Es schützt nicht automatisch die Ressourcen eines abonnierten Kontos.

Wenn Sie zu Ihrem AWS Firewall Manager Schutz eine Shield Advanced-Richtlinie verwenden, müssen Sie diesen Schritt nicht ausführen. Sie konfigurieren die Richtlinie mit den zu schützenden Ressourcentypen, und Firewall Manager fügt automatisch Schutzmaßnahmen zu Ressourcen hinzu, die in den Geltungsbereich der Richtlinie fallen.

Wenn Sie den Firewall Manager nicht verwenden, gehen Sie für jedes Konto, das über zu schützende Ressourcen verfügt, die folgenden Verfahren durch.

Um die Ressourcen auszuwählen, die mit Shield Advanced geschützt werden sollen

1. Wählen Sie auf der Seite zur Bestätigung des Abonnements des vorherigen Verfahrens oder auf der Seite Geschützte Ressourcen oder Übersicht die Option Zu schützende Ressourcen hinzufügen aus.
2. Geben Sie auf der Seite Ressourcen auswählen, die mit Shield Advanced geschützt werden sollen, unter Region und Ressourcentypen angeben die Regions- und Ressourcentypspezifikationen für die Ressourcen an, die Sie schützen möchten. Sie können Ressourcen in mehreren Regionen schützen, indem Sie Alle Regionen auswählen, und Sie können die Auswahl auf globale Ressourcen einschränken, indem Sie Global auswählen. Sie können alle Ressourcentypen abwählen, die Sie nicht schützen möchten. Informationen zum Schutz Ihrer Ressourcentypen finden Sie unter [AWS Shield Advanced Schutzmaßnahmen nach Ressourcentyp](#)
3. Wählen Sie Ressourcen laden aus. Shield Advanced füllt den Abschnitt Ressourcen auswählen mit den AWS Ressourcen, die Ihren Kriterien entsprechen.

4. Im Bereich Ressourcen auswählen können Sie die Ressourcenliste filtern, indem Sie eine Zeichenfolge eingeben, nach der in den Ressourcenlisten gesucht werden soll.

Wählen Sie die Ressourcen aus, die Sie schützen möchten.

5. Wenn Sie den von Ihnen erstellten Shield Advanced-Schutzmaßnahmen Tags hinzufügen möchten, geben Sie diese im Abschnitt Tags an. Informationen zum Markieren von AWS Ressourcen finden Sie unter [Arbeiten mit dem Tag-Editor](#).
6. Wählen Sie Protect with Shield Advanced. Dadurch werden die Ressourcen um Shield Advanced-Schutzmaßnahmen erweitert.

Fahren Sie mit den Bildschirmen des Konsolenassistenten fort, um die Konfiguration Ihres Ressourcenschutzes abzuschließen.

Themen

- [Konfigurieren Sie den DDoS-Schutz auf Anwendungsebene \(Schicht 7\) mit AWS WAF](#)
- [Konfigurieren Sie die gesundheitsbasierte Erkennung für Ihren Schutz](#)
- [Alarme und Benachrichtigungen konfigurieren](#)
- [Überprüfen und beenden Sie Ihre Schutzkonfiguration](#)

Konfigurieren Sie den DDoS-Schutz auf Anwendungsebene (Schicht 7) mit AWS WAF

Um eine Ressource auf Anwendungsebene zu schützen, verwendet Shield Advanced eine AWS WAF Web-ACL mit einer ratenbasierten Regel als Ausgangspunkt. AWS WAF ist eine Firewall für Webanwendungen, mit der Sie die HTTP- und HTTPS-Anfragen überwachen können, die an Ihre Ressourcen auf Anwendungsebene weitergeleitet werden, und mit der Sie den Zugriff auf Ihre Inhalte anhand der Eigenschaften der Anfragen steuern können. Eine ratenbasierte Regel begrenzt das Datenverkehrsvolumen auf der Grundlage Ihrer Anforderungsaggregationskriterien und bietet so einen grundlegenden DDoS-Schutz für Ihre Anwendung. Weitere Informationen finden Sie unter [Wie AWS WAF funktioniert](#) und [Ratenbasierte Regelnweisung](#).

Sie können optional auch die automatische DDoS-Abwehr von Shield Advanced auf Anwendungsebene aktivieren, sodass Shield Advanced-Ratenbegrenzungsanfragen von bekannten DDoS-Quellen erhalten und automatisch vorfallspezifische Schutzmaßnahmen für Sie bereitstellen.

⚠ Important

Wenn Sie Ihren Shield Advanced-Schutz AWS Firewall Manager mithilfe einer Shield Advanced-Richtlinie verwalten, können Sie den Schutz auf Anwendungsebene hier nicht verwalten. Sie müssen sie in Ihrer Firewall Manager Shield Advanced-Richtlinie verwalten.

Shield Advanced-Abonnements und AWS WAF Kosten

Ihr Shield Advanced-Abonnement deckt die Kosten für die Nutzung von AWS WAF Standardfunktionen für Ressourcen ab, die Sie mit Shield Advanced schützen. Die AWS WAF Standardgebühren, die durch Ihre Shield Advanced-Schutzmaßnahmen abgedeckt werden, sind die Kosten pro Web-ACL, die Kosten pro Regel und der Grundpreis pro Million Anfragen für die Prüfung von Webanfragen, bis zu 1.500 WCUs und bis zur Standardkörpergröße.

Durch die Aktivierung der automatischen DDoS-Abwehr auf Anwendungsebene von Shield Advanced wird Ihrer Web-ACL eine Regelgruppe hinzugefügt, die 150 Web-ACL-Kapazitätseinheiten (WCUs) verwendet. Diese WCUs werden auf die WCU-Nutzung in Ihrer Web-ACL angerechnet. Weitere Informationen finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#), [Die Shield Advanced-Regelgruppe](#) und [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#).

Ihr Abonnement AWS WAF für Shield Advanced deckt nicht die Nutzung von Ressourcen ab, die Sie nicht mit Shield Advanced schützen. Es deckt auch keine zusätzlichen, nicht standardmäßigen AWS WAF Kosten für geschützte Ressourcen ab. Beispiele für nicht standardmäßige AWS WAF Kosten sind die Kosten für Bot-Kontrolle, für CAPTCHA Regelaktionen, für Web-ACLs, die mehr als 1.500 WCUs verwenden, und für die Überprüfung des Anforderungstexts, der über die Standardgröße hinausgeht. Die vollständige Liste finden Sie auf der Seite mit den Preisen. AWS WAF

Vollständige Informationen und Preisbeispiele finden Sie unter [Shield Pricing](#) and [AWS WAF Pricing](#).

Um Layer-7-DDoS-Schutzmaßnahmen für eine Region zu konfigurieren

Shield Advanced bietet Ihnen die Möglichkeit, Layer-7-DDoS-Abwehr für jede Region zu konfigurieren, in der sich Ihre ausgewählten Ressourcen befinden. Wenn Sie Schutzmaßnahmen in mehreren Regionen hinzufügen, führt Sie der Assistent für jede Region durch das folgende Verfahren.

1. Auf der Seite Layer-7-DDoS-Schutz konfigurieren werden alle Ressourcen aufgeführt, die noch keiner Web-ACL zugeordnet sind. Wählen Sie für jede dieser Optionen entweder eine vorhandene Web-ACL aus oder erstellen Sie eine neue Web-ACL. Für jede Ressource, der


bereits eine Web-ACL zugeordnet ist, können Sie Web-ACLs ändern, indem Sie zuerst die Zuordnung der aktuellen ACL aufheben. AWS WAF Weitere Informationen finden Sie unter [Zuordnen oder Aufheben der Zuordnung einer Web-ACL zu einer Ressource AWS](#).

Für Web-ACLs, denen noch keine ratenbasierte Regel zugewiesen wurde, werden Sie vom Konfigurationsassistenten aufgefordert, eine hinzuzufügen. Eine ratenbasierte Regel begrenzt den Datenverkehr von IP-Adressen, wenn diese eine große Anzahl von Anfragen senden. Ratenbasierte Regeln schützen Ihre Anwendung vor einer Flut von Webanfragen und können Warnmeldungen über plötzliche Datenverkehrsspitzen ausgeben, die auf einen möglichen DDoS-Angriff hinweisen könnten. Fügen Sie einer Web-ACL eine ratenbasierte Regel hinzu, indem Sie Ratenbegrenzungsregel hinzufügen wählen und dann ein Ratenlimit und eine Regelaktion angeben. Sie können zusätzliche Schutzmaßnahmen in der Web-ACL über konfigurieren. AWS WAF

Informationen zur Verwendung von Web-ACLs und ratenbasierten Regeln in Ihren Shield Advanced-Schutzmaßnahmen, einschließlich zusätzlicher Konfigurationsoptionen für ratenbasierte Regeln, finden Sie unter [Shield Advanced AWS WAF Web-ACLs und ratenbasierte Regeln auf Anwendungsebene](#)

2. Wenn Sie möchten, dass Shield Advanced DDoS-Angriffe auf Ihre Ressourcen auf Anwendungsebene automatisch abwehrt, wählen Sie für Automatische DDoS-Abwehr auf Anwendungsebene Aktivieren und wählen Sie dann die AWS WAF Regelaktion aus, die Shield Advanced in seinen benutzerdefinierten Regeln verwenden soll. Diese Einstellung gilt für alle Web-ACLs für die Ressourcen, die Sie in dieser Assistentensitzung verwalten.

Mit automatischer DDoS-Abwehr auf Anwendungsebene verwaltet Shield Advanced eine ratenbasierte Regel in der AWS WAF Web-ACL der Ressource, die das Volumen der Anfragen von bekannten DDoS-Quellen begrenzt. Darüber hinaus vergleicht Shield Advanced aktuelle Verkehrsmuster mit historischen Verkehrsbasislinien, um Abweichungen zu erkennen, die auf einen DDoS-Angriff hinweisen könnten. Wenn Shield Advanced einen DDoS-Angriff erkennt, reagiert es darauf, indem es benutzerdefinierte AWS WAF Reaktionsregeln erstellt, auswertet und einsetzt. Sie geben an, ob die benutzerdefinierten Regeln Angriffe in Ihrem Namen zählen oder blockieren.

 Note

Die automatische DDoS-Abwehr auf Anwendungsebene funktioniert nur mit Web-ACLs, die mit der neuesten Version von AWS WAF (v2) erstellt wurden.

Weitere Informationen zur automatischen DDoS-Abwehr von Shield Advanced auf Anwendungsebene, einschließlich Vorbehalte und Best Practices für die Verwendung dieser Funktion, finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#)

3. Wählen Sie Weiter aus. Der Konsolenassistent wechselt zur Seite für die systembasierte Erkennung.

Konfigurieren Sie die gesundheitsbasierte Erkennung für Ihren Schutz

Konfigurieren Sie Shield Advanced so, dass es eine auf Integrität basierende Erkennung verwendet, um die Reaktionsfähigkeit und Genauigkeit bei der Erkennung und Abwehr von Angriffen zu verbessern. Gut konfigurierte Integritätsprüfungen sind für die genaue Erkennung von Ereignissen unerlässlich. Sie können die zustandsbasierte Erkennung für jeden Ressourcentyp mit Ausnahme von Route 53-Hosting-Zonen konfigurieren.

Um die gesundheitsbasierte Erkennung zu verwenden, definieren Sie eine Zustandsprüfung für Ihre Ressource in Route 53 und verknüpfen Sie die Zustandsprüfung dann mit Ihrem Shield Advanced-Schutz. Es ist wichtig, dass die von Ihnen konfigurierte Zustandsprüfung den Zustand der Ressource genau widerspiegelt. Informationen und Beispiele für die Konfiguration von Integritätsprüfungen zur Verwendung mit Shield Advanced finden Sie unter [Gesundheitsbasierte Erkennung mithilfe von Gesundheitschecks](#).


Für den proaktiven Engagement-Support des Shield Response Teams (SRT) sind Gesundheitschecks erforderlich. Informationen zu proaktivem Engagement finden Sie unter [Konfiguration von proaktivem Engagement](#).

Note

Gesundheitschecks müssen als fehlerfrei gemeldet werden, wenn Sie sie mit Ihren Shield Advanced-Schutzmaßnahmen verknüpfen.

So konfigurieren Sie die zustandsbasierte Erkennung

1. Wählen Sie unter Associated Health Check (Zugehörige Zustandsprüfung) die ID der Zustandsprüfung aus, die Sie der Schutzvorkehrung zuordnen möchten.

 Note

Wenn Sie die benötigte Zustandsprüfung nicht sehen, rufen Sie die Route 53-Konsole auf und überprüfen Sie die Zustandsprüfung und ihre ID. Weitere Informationen finden Sie unter [Erstellen und Aktualisieren von Zustandsprüfungen](#).

2. Wählen Sie Weiter aus. Der Konsolenassistent wechselt zur Seite mit Alarmen und Benachrichtigungen.

Alarme und Benachrichtigungen konfigurieren

Sie können optional Amazon Simple Notification Service-Benachrichtigungen für erkannte CloudWatch Amazon-Alarme und ratenbasierte Regelaktivitäten konfigurieren. Sie können diese verwenden, um Benachrichtigungen zu erhalten, wenn Shield ein Ereignis auf einer geschützten Ressource erkennt oder wenn ein in einer ratenbasierten Regel konfiguriertes Ratenlimit überschritten wird.

Informationen zu Shield CloudWatch Advanced-Metriken finden Sie unter [AWS Shield Advanced Metriken](#). Informationen zu Amazon SNS finden Sie im [Amazon Simple Notification Service Developer Guide](#).

Um Alarme und Benachrichtigungen zu konfigurieren

1. Wählen Sie die Amazon SNS SNS-Themen aus, für die Sie eine Benachrichtigung wünschen. Sie können ein einzelnes Amazon SNS SNS-Thema für alle geschützten Ressourcen und ratenbasierten Regeln verwenden, oder Sie können verschiedene Themen wählen, die auf Ihre Organisation zugeschnitten sind. Sie können beispielsweise ein SNS-Thema für jedes Team erstellen, das für die Reaktion auf Vorfälle für eine bestimmte Gruppe von Ressourcen verantwortlich ist.
2. Wählen Sie Weiter aus. Der Konsolenassistent wechselt zur Seite mit der Überprüfung des Ressourcenschutzes.

Überprüfen und beenden Sie Ihre Schutzkonfiguration

Um Ihre Einstellungen zu überprüfen und zu konfigurieren

1. Überprüfen Sie auf der Seite DDoS-Abwehr und Sichtbarkeit, ob Sie die Sichtbarkeit überprüfen und konfigurieren Ihre Einstellungen. Um Änderungen vorzunehmen, wählen Sie in dem Bereich, den Sie ändern möchten, die Option Bearbeiten aus. Dadurch kehren Sie zur entsprechenden Seite im Konsolenassistenten zurück. Nehmen Sie Ihre Änderungen vor und klicken Sie dann auf den folgenden Seiten auf Weiter, bis Sie zur Seite DDoS-Abwehr und Sichtbarkeit überprüfen und konfigurieren zurückkehren.
2. Wählen Sie Konfiguration beenden aus. Auf der Seite Geschützte Ressourcen werden Ihre neu geschützten Ressourcen aufgeführt.

AWS SRT-Unterstützung konfigurieren

Das Shield Response Team (SRT) besteht aus Sicherheitsingenieuren, die sich auf die Reaktion auf DDoS-Ereignisse spezialisiert haben. Sie können optional Berechtigungen hinzufügen, die es dem SRT ermöglichen, während eines DDoS-Ereignisses Ressourcen in Ihrem Namen zu verwalten. Darüber hinaus können Sie das SRT so konfigurieren, dass es proaktiv mit Ihnen Kontakt aufnimmt, falls die Route 53-Zustandsprüfungen, die mit Ihren geschützten Ressourcen verknüpft sind, während eines erkannten Ereignisses fehlerhaft sind. Diese beiden Erweiterungen Ihres Schutzes ermöglichen schnellere Reaktionen auf DDoS-Ereignisse.

Note

Um die Dienste des Shield Response Teams (SRT) nutzen zu können, müssen Sie den [Business Support Plan oder den Enterprise Support Plan](#) abonniert haben.

Das SRT kann AWS WAF Anforderungsdaten und Protokolle bei Ereignissen auf Anwendungsebene überwachen, um anomalen Datenverkehr zu identifizieren. Sie können dabei helfen, benutzerdefinierte AWS WAF Regeln zu erstellen, um schädliche Datenverkehrsquellen einzudämmen. Bei Bedarf kann das SRT architektonische Empfehlungen aussprechen, damit Sie Ihre Ressourcen besser an den Empfehlungen ausrichten können. AWS

Weitere Informationen zum SRT finden Sie unter [Unterstützung durch das Shield Response Team \(SRT\)](#)

Um dem SRT Berechtigungen zu erteilen

1. Wählen Sie auf der Übersichtsseite der AWS Shield Konsole unter **AWS SRT-Unterstützung** konfigurieren die Option **SRT-Zugriff bearbeiten** aus. Die Zugriffsseite für das AWS Shield Response Team (SRT) bearbeiten wird geöffnet.
2. Wählen Sie für die Einstellung für den SRT-Zugriff eine der folgenden Optionen aus:
 - Gewähren Sie dem SRT keinen Zugriff auf mein Konto — Shield entfernt alle Berechtigungen, die Sie dem SRT zuvor für den Zugriff auf Ihr Konto und Ihre Ressourcen erteilt haben.
 - Eine neue Rolle für das SRT erstellen, um auf mein Konto zuzugreifen — Shield erstellt eine Rolle, die dem Service Principal `drt.shield.amazonaws.com`, der das SRT darstellt, vertraut, und fügt ihm die verwaltete Richtlinie hinzu. `AWSShieldDRTAccessPolicy` Die verwaltete Richtlinie ermöglicht es dem SRT, in Ihrem Namen AWS WAF API-Aufrufe zu tätigen AWS Shield Advanced und auf Ihre Protokolle zuzugreifen. AWS WAF Für weitere Informationen über die verwaltete Richtlinie siehe [AWS verwaltete Richtlinie: AWSShieldDRTAccessPolicy](#).
 - Wählen Sie eine bestehende Rolle für das SRT aus, um auf meine Konten zuzugreifen. Für diese Option müssen Sie die Konfiguration der Rolle in AWS Identity and Access Management (IAM) wie folgt ändern:
 - Hängen Sie die verwaltete Richtlinie `AWSShieldDRTAccessPolicy` an die Rolle an. Diese verwaltete Richtlinie ermöglicht es dem SRT, in Ihrem Namen AWS WAF API-Aufrufe zu tätigen AWS Shield Advanced und auf Ihre Protokolle zuzugreifen. AWS WAF Für weitere Informationen über die verwaltete Richtlinie siehe [AWS verwaltete Richtlinie: AWSShieldDRTAccessPolicy](#). Informationen zum Anhängen der verwalteten Richtlinie an Ihre Rolle finden Sie unter IAM-Richtlinien [anhängen und trennen](#).
 - Ändern Sie die Rolle, um dem Service-Prinzipal `drt.shield.amazonaws.com` zu vertrauen. Dies ist der Dienstprinzipal, der die SRT repräsentiert. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: Prinzipal](#).
3. Wählen Sie **Speichern**, um Ihre Änderungen zu speichern.

Weitere Informationen darüber, wie Sie dem SRT Zugriff auf Ihre Schutzmaßnahmen und Daten gewähren, finden Sie unter [Konfiguration des Zugriffs für das Shield Response Team \(SRT\)](#)

Um den proaktiven Einsatz von SRT zu ermöglichen

1. Wählen Sie auf der Übersichtsseite der AWS Shield Konsole unter Proaktive Interaktion und Kontakte im Bereich Kontakte die Option Bearbeiten aus.

Geben Sie auf der Seite Kontakte bearbeiten die Kontaktinformationen der Personen ein, die das SRT für proaktive Interaktionen kontaktieren soll.

Wenn Sie mehr als einen Kontakt angeben, geben Sie in den Anmerkungen an, unter welchen Umständen jeder Kontakt verwendet werden soll. Geben Sie die Namen der primären und sekundären Kontaktpersonen an und geben Sie die Verfügbarkeitszeiten und Zeitzonen für jeden Kontakt an.

Beispiele für Kontaktnotizen:

- Dies ist eine Hotline, die rund um die Uhr besetzt ist. Bitte arbeiten Sie mit dem antwortenden Analysten zusammen und er wird die entsprechende Person für das Gespräch finden.
- Bitte kontaktieren Sie mich, wenn die Hotline nicht innerhalb von 5 Minuten antwortet.

2. Wählen Sie Speichern.

Die Übersichtsseite enthält die aktualisierten Kontaktinformationen.

3. Wählen Sie die Funktion „Proaktive Interaktion bearbeiten“, dann „Aktivieren“ und anschließend „Speichern“, um die proaktive Interaktion zu aktivieren.

Weitere Informationen zu proaktivem Engagement finden Sie unter [Konfiguration von proaktivem Engagement](#).

Erstellen Sie ein DDoS-Dashboard CloudWatch und stellen Sie Alarme ein CloudWatch

Sie können potenzielle DDoS-Aktivitäten mithilfe von Amazon überwachen. Amazon CloudWatch sammelt Rohdaten von Shield Advanced und verarbeitet sie zu lesbaren Metriken, die nahezu in Echtzeit verfügbar sind. Mithilfe von Statistiken können Sie CloudWatch sich einen Überblick über die Leistung Ihrer Webanwendung oder Ihres Dienstes verschaffen. Weitere Informationen zur Verwendung CloudWatch finden Sie unter [Was ist CloudWatch](#) im CloudWatch Amazon-Benutzerhandbuch enthalten.

- Anweisungen zum Erstellen eines CloudWatch Dashboards finden Sie unter [Überwachung mit Amazon CloudWatch](#).
- Eine Beschreibung der Shield Advanced-Metriken, die Sie Ihrem Dashboard hinzufügen können, finden Sie unter [AWS Shield Advanced Metriken](#).

Shield Advanced meldet Ressourcenmetriken CloudWatch häufiger bei DDoS-Ereignissen als wenn keine Ereignisse im Gange sind. Shield Advanced meldet Metriken einmal pro Minute während eines Ereignisses und dann einmal direkt nach dem Ende des Ereignisses. Solange keine Ereignisse im Gange sind, meldet Shield Advanced Metriken einmal täglich zu einer der Ressource zugewiesenen Zeit. Dieser regelmäßige Bericht sorgt dafür, dass die Messwerte aktiv sind und in Ihren benutzerdefinierten CloudWatch Alarmen verwendet werden können.

Damit ist das Tutorial für die ersten Schritte mit Shield Advanced abgeschlossen. Erkunden Sie die Funktionen und Optionen von Shield Advanced weiter, um die Vorteile der von Ihnen ausgewählten Schutzmaßnahmen voll auszuschöpfen. Machen Sie sich zunächst mit Ihren Optionen für die Anzeige und Reaktion auf Ereignisse bei [Einblick in DDoS-Ereignisse](#) und [Reagieren auf DDoS-Ereignisse](#) vertraut.

Unterstützung durch das Shield Response Team (SRT)

Das Shield Response Team (SRT) bietet zusätzlichen Support für Shield Advanced-Kunden. Die SRT sind Sicherheitsingenieure, die sich auf die Reaktion auf DDoS-Ereignisse spezialisiert haben. Als zusätzliche Unterstützungsebene zu Ihrem AWS Support Plan können Sie direkt mit den SRT zusammenarbeiten und deren Fachwissen als Teil Ihres Workflows zur Reaktion auf Ereignisse nutzen. Informationen zu den Optionen und Anleitungen zur Konfiguration finden Sie in den folgenden Themen.

Note

Um die Dienste des Shield Response Teams (SRT) nutzen zu können, müssen Sie den [Business Support Plan oder den Enterprise Support Plan](#) abonniert haben.

SRT-Supportaktivitäten

Das Hauptziel einer Zusammenarbeit mit der SRT besteht darin, die Verfügbarkeit und Leistung Ihrer Anwendung zu schützen. Abhängig von der Art des DDoS-Ereignisses und der Architektur Ihrer Anwendung kann das SRT eine oder mehrere der folgenden Maßnahmen ergreifen:

- **AWS WAF Protokollanalyse und Regeln** — Bei Ressourcen, die eine AWS WAF Web-ACL verwenden, kann das SRT Ihre AWS WAF Protokolle analysieren, um Angriffsmerkmale in Ihren Anwendungs-Webanfragen zu identifizieren. Mit Ihrer Zustimmung während des Einsatzes kann das SRT Änderungen an Ihrer Web-ACL vornehmen, um die identifizierten Angriffe zu blockieren.
- **Erstellen Sie benutzerdefinierte Abwehrmaßnahmen für Ihr Netzwerk** — Das SRT kann für Sie maßgeschneiderte Abhilfemaßnahmen für Angriffe auf Infrastrukturebene erstellen. Das SRT kann mit Ihnen zusammenarbeiten, um den für Ihre Anwendung zu erwartenden Datenverkehr zu verstehen, unerwarteten Datenverkehr zu blockieren und die Geschwindigkeitsbegrenzungen für Pakete pro Sekunde zu optimieren. Weitere Informationen finden Sie unter [Konfiguration benutzerdefinierter Abhilfemaßnahmen mit dem Shield Response Team \(SRT\)](#).
- **Netzwerkverkehrstechnik** — Das SRT arbeitet eng mit AWS Netzwerkteams zusammen, um Shield Advanced-Kunden zu schützen. AWS kann bei Bedarf die Art und Weise ändern, wie Internetverkehr im AWS Netzwerk ankommt, um Ihrer Anwendung mehr Kapazität zur Schadensbegrenzung zuzuweisen.
- **Empfehlungen zur Architektur** — Das SRT kann feststellen, dass die beste Abwehr eines Angriffs Architekturänderungen erfordert, um sie besser an den AWS bewährten Methoden auszurichten, und diese helfen Ihnen bei der Implementierung dieser Verfahren. Weitere Informationen finden Sie unter [AWS Bewährte Methoden für DDoS-Resilienz](#).

Themen

- [Konfiguration des Zugriffs für das Shield Response Team \(SRT\)](#)
- [Konfiguration von proaktivem Engagement](#)
- [Das Shield Response Team \(SRT\) kontaktieren](#)
- [Konfiguration benutzerdefinierter Abhilfemaßnahmen mit dem Shield Response Team \(SRT\)](#)

Konfiguration des Zugriffs für das Shield Response Team (SRT)

Sie können dem Shield Response Team (SRT) die Erlaubnis erteilen, in Ihrem Namen zu handeln, auf Ihre AWS WAF Protokolle zuzugreifen und Aufrufe an die AWS Shield Advanced und AWS WAF APIs zu tätigen, um Schutzmaßnahmen zu verwalten. Bei DDoS-Ereignissen auf Anwendungsebene kann das SRT AWS WAF Anfragen überwachen, um anomalen Datenverkehr zu identifizieren und dabei zu helfen, benutzerdefinierte AWS WAF Regeln zur Abwehr anstößiger Datenverkehrsquellen zu erstellen.

Darüber hinaus können Sie dem SRT Zugriff auf andere Daten gewähren, die Sie in Amazon S3 S3-Buckets gespeichert haben, z. B. Paketerfassungen oder Protokolle von einem Application Load Balancer CloudFront, Amazon oder aus Quellen von Drittanbietern.


Note

Um die Dienste des Shield Response Teams (SRT) nutzen zu können, müssen Sie den [Business Support Plan oder den Enterprise Support Plan](#) abonniert haben.

Um die Berechtigungen für das SRT zu verwalten

1. Wählen Sie auf der Übersichtsseite der AWS Shield Konsole unter **AWS SRT-Unterstützung** konfigurieren die Option **SRT-Zugriff bearbeiten** aus. Die Zugriffsseite für das AWS Shield Response Team (SRT) bearbeiten wird geöffnet.
2. Wählen Sie für die Einstellung für den SRT-Zugriff eine der folgenden Optionen aus:
 - Gewähren Sie dem SRT keinen Zugriff auf mein Konto — Shield entfernt alle Berechtigungen, die Sie dem SRT zuvor für den Zugriff auf Ihr Konto und Ihre Ressourcen erteilt haben.
 - Eine neue Rolle für das SRT erstellen, um auf mein Konto zuzugreifen — Shield erstellt eine Rolle, die dem Service `Principal::shield.amazonaws.com`, der das SRT darstellt, vertraut, und fügt ihm die verwaltete Richtlinie hinzu. `AWSShieldDRTAccessPolicy` Die verwaltete Richtlinie ermöglicht es dem SRT, in Ihrem Namen AWS WAF API-Aufrufe zu tätigen AWS Shield Advanced und auf Ihre Protokolle zuzugreifen. AWS WAF Für weitere Informationen über die verwaltete Richtlinie siehe [AWS verwaltete Richtlinie: AWSShieldDRTAccessPolicy](#).
 - Wählen Sie eine bestehende Rolle für das SRT aus, um auf meine Konten zuzugreifen. Für diese Option müssen Sie die Konfiguration der Rolle in AWS Identity and Access Management (IAM) wie folgt ändern:
 - Hängen Sie die verwaltete Richtlinie `AWSShieldDRTAccessPolicy` an die Rolle an. Diese verwaltete Richtlinie ermöglicht es dem SRT, in Ihrem Namen AWS WAF API-Aufrufe zu tätigen AWS Shield Advanced und auf Ihre Protokolle zuzugreifen. AWS WAF Für weitere Informationen über die verwaltete Richtlinie siehe [AWS verwaltete Richtlinie: AWSShieldDRTAccessPolicy](#). Informationen zum Anhängen der verwalteten Richtlinie an Ihre Rolle finden Sie unter IAM-Richtlinien [anhängen und trennen](#).

- Ändern Sie die Rolle, um dem Service-Prinzipal `drt.shield.amazonaws.com` zu vertrauen. Dies ist der Dienstprinzipal, der die SRT repräsentiert. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: Prinzipal](#).
3. Für (optional): Gewähren Sie SRT-Zugriff auf einen Amazon S3-Bucket. Wenn Sie Daten teilen müssen, die nicht in Ihren AWS WAF Web-ACL-Protokollen enthalten sind, konfigurieren Sie dies. Zum Beispiel Application Load Balancer Balancer-Zugriffsprotokolle, CloudFront Amazon-Protokolle oder Protokolle aus Quellen von Drittanbietern.

 Note

Sie müssen dies nicht für Ihre AWS WAF Web-ACL-Protokolle tun. Das SRT erhält Zugriff auf diese, wenn Sie Zugriff auf Ihr Konto gewähren.

- a. Konfigurieren Sie die Amazon S3 S3-Buckets gemäß den folgenden Richtlinien:
- Die Bucket-Standorte müssen sich in dem befinden AWS-Konto , auf den Sie dem SRT im vorherigen Schritt Zugriff auf das AWS Shield Response Team (SRT) gewährt haben.
 - Die Buckets können entweder Klartext- oder SSE-S3-verschlüsselt sein. Weitere Informationen zur Amazon S3 SSE-S3-Verschlüsselung finden Sie unter [Schützen von Daten mithilfe serverseitiger Verschlüsselung mit Amazon S3-Managed Encryption Keys \(SSE-S3\) im Amazon S3 S3-Benutzerhandbuch](#).

Das SRT kann keine Protokolle anzeigen oder verarbeiten, die in Buckets gespeichert sind, die mit Schlüsseln verschlüsselt sind, die in () gespeichert sind. AWS Key Management Service AWS KMS

- b. Geben Sie im Abschnitt Shield Advanced (optional): SRT-Zugriff auf einen Amazon S3-Bucket für jeden Amazon S3-Bucket, in dem Ihre Daten oder Logs gespeichert sind, den Namen des Buckets ein und wählen Sie Bucket hinzufügen. Sie können bis zu 10 Buckets hinzufügen.

Dadurch erhält das SRT die folgenden Berechtigungen für jeden Bucket:`s3:GetBucketLocation,s3:GetObject`, und. `s3:ListBucket`

Wenn Sie dem SRT die Erlaubnis geben möchten, auf mehr als 10 Buckets zuzugreifen, können Sie dies tun, indem Sie die zusätzlichen Bucket-Richtlinien bearbeiten und die hier aufgeführten Berechtigungen für das SRT manuell gewähren.

Im Folgenden finden Sie ein Beispiel für eine Richtlinienliste.

```
{
  "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. Wählen Sie Speichern, um Ihre Änderungen zu speichern.

[Sie können das SRT auch über die API autorisieren, indem Sie eine IAM-Rolle erstellen, ihr die Richtlinie anhängen und die Rolle dann AWSShieldDRTAccessPolicy an den Vorgang AssociatedRtRole übergeben.](#)

Konfiguration von proaktivem Engagement

Bei proaktivem Engagement kontaktiert Sie das Shield Response Team (SRT) direkt, wenn die Verfügbarkeit oder Leistung Ihrer Anwendung aufgrund eines möglichen Angriffs beeinträchtigt wird. Wir empfehlen dieses Einsatzmodell, da es die schnellste SRT-Reaktion bietet und es dem SRT ermöglicht, mit der Fehlerbehebung zu beginnen, noch bevor es Kontakt mit Ihnen aufgenommen hat.

Proaktives Engagement ist für Ereignisse auf Netzwerk- und Transportebene auf Elastic IP-Adressen und AWS Global Accelerator Standardbeschleunigern sowie für Webanforderungsfluten auf CloudFront Amazon-Distributionen und Application Load Balancern verfügbar. Proaktives Engagement ist nur für Shield Advanced-Ressourcenschutzmaßnahmen verfügbar, denen eine Amazon Route 53-Zustandsprüfung zugeordnet ist. Informationen zur Verwaltung und Verwendung von Integritätsprüfungen finden Sie unter [Gesundheitsbasierte Erkennung mithilfe von Gesundheitschecks](#).

Während eines Ereignisses, das von Shield Advanced erkannt wird, verwendet das SRT den Status Ihrer Gesundheitschecks, um festzustellen, ob das Ereignis für ein proaktives Eingreifen in Frage kommt. In diesem Fall wird sich das SRT gemäß den Kontaktangaben, die Sie in Ihrer Konfiguration für proaktives Engagement angegeben haben, mit Ihnen in Verbindung setzen.

Sie können bis zu zehn Kontakte für proaktives Engagement konfigurieren und Sie können Hinweise angeben, die das SRT bei der Kontaktaufnahme mit Ihnen unterstützen. Ihre Ansprechpartner für proaktives Engagement sollten verfügbar sein, um während Veranstaltungen mit dem SRT in Kontakt zu treten. Wenn Sie nicht über ein rund um die Uhr verfügbares Betriebszentrum verfügen, können Sie einen Pager-Kontakt angeben und diese Kontaktpräferenz in Ihren Kontaktnotizen angeben.

Für ein proaktives Engagement müssen Sie Folgendes tun:

- Sie müssen den [Business Support Plan oder den Enterprise Support Plan](#) abonniert haben.
- Sie müssen jeder Ressource, die Sie durch proaktives Engagement schützen möchten, eine Amazon Route 53-Zustandsprüfung zuordnen. Das SRT verwendet den Status Ihrer Zustandsprüfungen, um festzustellen, ob ein Ereignis ein proaktives Eingreifen erfordert. Daher ist es wichtig, dass Ihre Zustandsprüfungen den Status Ihrer geschützten Ressourcen genau widerspiegeln. Weitere Informationen und Anleitungen finden Sie unter [Gesundheitsbasierte Erkennung mithilfe von Gesundheitschecks](#).
- Für eine Ressource, der eine AWS WAF Web-ACL zugeordnet ist, müssen Sie die Web-ACL mit AWS WAF (v2) erstellen, der neuesten Version von AWS WAF.
- Sie müssen mindestens einen Ansprechpartner angeben, den das SRT für proaktive Interaktionen während einer Veranstaltung nutzen kann. Halten Sie Ihre Kontaktinformationen vollständig und aktuell.

Um ein proaktives Engagement von SRT zu ermöglichen

1. Wählen Sie auf der Übersichtsseite der AWS Shield Konsole unter Proaktive Interaktion und Kontakte im Bereich Kontakte die Option Bearbeiten aus.

Geben Sie auf der Seite Kontakte bearbeiten die Kontaktinformationen der Personen ein, die das SRT für proaktive Interaktionen kontaktieren soll.

Wenn Sie mehr als einen Kontakt angeben, geben Sie in den Anmerkungen an, unter welchen Umständen jeder Kontakt verwendet werden soll. Geben Sie die Namen der primären und sekundären Kontaktpersonen an und geben Sie die Verfügbarkeitszeiten und Zeitzonen für jeden Kontakt an.

Beispiele für Kontaktnotizen:

- Dies ist eine Hotline, die rund um die Uhr besetzt ist. Bitte arbeiten Sie mit dem antwortenden Analysten zusammen und er wird die entsprechende Person für das Gespräch finden.
- Bitte kontaktieren Sie mich, wenn die Hotline nicht innerhalb von 5 Minuten antwortet.

2. Wählen Sie Speichern.

Die Übersichtsseite enthält die aktualisierten Kontaktinformationen.

3. Wählen Sie die Funktion „Proaktive Interaktion bearbeiten“, dann „Aktivieren“ und anschließend „Speichern“, um die proaktive Interaktion zu aktivieren.

Das Shield Response Team (SRT) kontaktieren

Sie können das Shield Response Team (SRT) auf eine der folgenden Arten kontaktieren:

Support-Fall

Sie können einen Fall unter AWS Shield in der AWS Support Center-Konsole öffnen.

Anleitungen zur Erstellung eines Support-Falls finden Sie [AWS Support im Center](#).

Wählen Sie den Schweregrad aus, der Ihrer Situation entspricht, und geben Sie Ihre Kontaktdaten an. Geben Sie in der Beschreibung so viele Details wie möglich an. Geben Sie Informationen zu allen geschützten Ressourcen an, von denen Sie glauben, dass sie betroffen sein könnten, sowie zum aktuellen Stand Ihrer Endbenutzererfahrung. Wenn beispielsweise Ihre Benutzererfahrung beeinträchtigt ist oder Teile Ihrer Anwendung derzeit nicht verfügbar sind, geben Sie diese Informationen an.

- Bei vermuteten DDoS-Angriffen — Wenn die Verfügbarkeit oder Leistung Ihrer Anwendung derzeit durch einen möglichen DDoS-Angriff beeinträchtigt wird, wählen Sie den folgenden Schweregrad und die folgenden Kontaktoptionen aus:
 - Wählen Sie für den Schweregrad den höchsten Schweregrad, der für Ihren Supportplan verfügbar ist:
 - Für Business-Support ist das Produktionssystem ausgefallen: < 1 Stunde.
 - Für Enterprise-Support ist dies ein Ausfall des geschäftskritischen Systems: < 15 Minuten.
 - Wählen Sie als Kontaktoption entweder Telefon oder Chat und geben Sie Ihre Daten ein. Die Verwendung einer Live-Kontaktmethode bietet die schnellste Antwort.

Proaktives Engagement

Bei AWS Shield Advanced proaktivem Einsatz kontaktiert das SRT Sie direkt, wenn der Amazon Route 53-Zustandstest, der mit Ihrer geschützten Ressource verknüpft ist, während eines erkannten Ereignisses fehlerhaft wird. Weitere Informationen zu dieser Option finden Sie unter [Konfiguration von proaktivem Engagement](#).

Konfiguration benutzerdefinierter Abhilfemaßnahmen mit dem Shield Response Team (SRT)

Für Ihre Elastic IPs (EIPs) und Ihre AWS Global Accelerator Standard-Accelerators können Sie mit dem Shield Response Team (SRT) zusammenarbeiten, um benutzerdefinierte Abhilfemaßnahmen zu konfigurieren. Dies ist nützlich, falls Sie eine bestimmte Logik kennen, die bei der Einführung einer Risikominderung durchgesetzt werden sollte. Beispielsweise möchten Sie möglicherweise nur Datenverkehr aus bestimmten Ländern zulassen, bestimmte Ratenbegrenzungen durchsetzen, optionale Validierungen konfigurieren, Fragmente nicht zulassen oder nur Datenverkehr zulassen, der einem bestimmten Muster in der Paketnutzlast entspricht.

Zu den häufigsten benutzerdefinierten Abhilfemaßnahmen gehören die folgenden:

- **Musterabgleich** — Wenn Sie einen Dienst betreiben, der mit clientseitigen Anwendungen interagiert, können Sie sich für den Abgleich nach bekannten Mustern entscheiden, die für diese Anwendungen spezifisch sind. Sie können beispielsweise einen Spiel- oder Kommunikationsdienst betreiben, bei dem der Endbenutzer bestimmte Software installieren muss, die Sie vertreiben. Sie können jedem Paket, das von der Anwendung an Ihren Dienst gesendet wird, eine magische Zahl hinzufügen. Sie können bis zu 128 Byte (getrennt oder zusammenhängend) einer nicht fragmentierten Nutzlast und Header eines nicht fragmentierten TCP- oder UDP-Pakets zuordnen. Die Übereinstimmung kann in hexadezimaler Schreibweise als spezifischer Offset vom Anfang der Paketnutzlast oder als dynamischer Offset nach einem bekannten Wert ausgedrückt werden. Die Schadensbegrenzung kann beispielsweise nach dem Byte suchen `0x01` und dann die nächsten vier Byte erwarten `0x12345678`.
- **DNS-spezifisch** — Wenn Sie Ihren eigenen autoritativen DNS-Service mit Diensten wie Global Accelerator oder Amazon Elastic Compute Cloud (Amazon EC2) betreiben, können Sie eine benutzerdefinierte Schadensbegrenzung anfordern, die Pakete validiert, um sicherzustellen, dass es sich um gültige DNS-Abfragen handelt, und eine Verdachtsbewertung anwenden, bei der Attribute ausgewertet werden, die spezifisch für den DNS-Verkehr sind.

Wenn Sie sich über die Zusammenarbeit mit SRT bei der Erstellung benutzerdefinierter Abhilfemaßnahmen erkundigen möchten, erstellen Sie einen Support-Fall unter [AWS Shield Weitere Informationen zum Erstellen von AWS Support Fällen](#) finden Sie unter [Erste Schritte](#) mit [AWS Support](#)

Ressourcenschutz in AWS Shield Advanced

Sie können AWS Shield Advanced Schutzmaßnahmen für Ihre Ressourcen hinzufügen und konfigurieren. Sie können den Schutz für eine einzelne Ressource verwalten und Ihre geschützten Ressourcen zur besseren Verwaltung von Ereignissen in logischen Sammlungen gruppieren. Sie können Änderungen an Ihren Shield Advanced-Schutzmaßnahmen auch mit AWS Config verfolgen.

Themen

- [AWS Shield Advanced Schutzmaßnahmen nach Ressourcentyp](#)
- [AWS Shield Advanced Schutzmaßnahmen auf Anwendungsebene \(Schicht 7\)](#)
- [Gesundheitsbasierte Erkennung mithilfe von Gesundheitschecks](#)
- [Verwaltung des Ressourcenschutzes in AWS Shield Advanced](#)
- [AWS Shield Advanced Schutzgruppen](#)
- [Verfolgung von Änderungen am Ressourcenschutz in AWS Config](#)

AWS Shield Advanced Schutzmaßnahmen nach Ressourcentyp

Shield Advanced schützt AWS Ressourcen in der Netzwerk- und Transportebene (Schichten 3 und 4) und in der Anwendungsschicht (Schicht 7). Sie können einige Ressourcen direkt und andere durch die Verknüpfung mit geschützten Ressourcen schützen. Shield Advanced unterstützt IPv4 und IPv6 nicht.

Dieser Abschnitt enthält Informationen zu Shield Advanced-Schutzmaßnahmen für jeden Ressourcentyp.

Note

Shield Advanced schützt nur Ressourcen, die Sie entweder in Shield Advanced oder durch eine AWS Firewall Manager Shield Advanced-Richtlinie angegeben haben. Ihre Ressourcen werden nicht automatisch geschützt.

Sie können Shield Advanced für erweiterte Überwachung und Schutz mit den folgenden Ressourcentypen verwenden:

- CloudFront Amazon-Distributionen. Für CloudFront eine kontinuierliche Bereitstellung schützt Shield Advanced jede Staging-Distribution, die einer geschützten Primärdistribution zugeordnet ist.
- Gehostete Zonen von Amazon Route 53.
- AWS Global Accelerator Standardbeschleuniger.
- Amazon EC2 Elastic IP-Adressen. Shield Advanced schützt die Ressourcen, die geschützten Elastic IP-Adressen zugeordnet sind.
- Amazon EC2-Instances durch Zuordnung zu Amazon EC2 Elastic IP-Adressen.
- Die folgenden Elastic Load Balancing (ELB) -Load Balancer:
 - Load Balancer für Anwendungen.
 - Classic Load Balancer.
 - Network Load Balancers über Verknüpfungen zu Amazon EC2 Elastic IP-Adressen.

Sie können Shield Advanced nicht verwenden, um andere Ressourcentypen zu schützen. Sie können beispielsweise keine AWS Global Accelerator benutzerdefinierten Routing-Beschleuniger oder Gateway Load Balancer schützen.

Sie können pro Ressourcentyp bis zu 1.000 Ressourcen überwachen und schützen. AWS-Konto In einem einzigen Konto könnten Sie beispielsweise 1.000 Amazon EC2 Elastic IP-Adressen, 1.000 CloudFront Distributionen und 1.000 Application Load Balancer schützen. Sie können eine Erhöhung der Anzahl der Ressourcen, die Sie mit Shield Advanced schützen können, über die Service Quotas Quota-Konsole unter <https://console.aws.amazon.com/servicequotas/> beantragen.

Schutz von Amazon EC2 EC2-Instances und Network Load Balancers mit Shield Advanced

Sie können Amazon EC2 EC2-Instances und Network Load Balancers schützen, indem Sie diese Ressourcen zuerst an Elastic IP-Adressen anhängen und dann die Elastic IP-Adressen in Shield Advanced schützen.

Wenn Sie Elastic IP-Adressen schützen, identifiziert und schützt Shield Advanced die Ressourcen, mit denen sie verknüpft sind. Shield Advanced identifiziert automatisch den Ressourcentyp, der an eine Elastic IP-Adresse angehängt ist, und wendet die entsprechenden Erkennungen und Abhilfemaßnahmen für diese Ressource an. Dazu gehört die Konfiguration von Netzwerk-ACLs, die für die Elastic IP-Adresse spezifisch sind. Weitere Informationen zur Verwendung von Elastic

IP-Adressen mit Ihren AWS Ressourcen finden Sie in den folgenden Anleitungen: [Amazon Elastic Compute Cloud-Dokumentation](#) oder [Elastic Load Balancing Balancing-Dokumentation](#).

Während eines Angriffs verteilt Shield Advanced Ihre Netzwerk-ACLs automatisch an der Netzwerkgrenze. AWS Wenn sich Ihre Netzwerk-ACLs an der Netzwerkgrenze befinden, kann Shield Advanced Schutz vor größeren DDoS-Ereignissen bieten. In der Regel werden Netzwerk-ACLs in der Nähe Ihrer Amazon EC2 EC2-Instances innerhalb Ihrer Amazon VPC angewendet. Die Netzwerk-ACL kann Angriffe nur so groß abwehren, wie Ihre Amazon VPC und Instance handhaben können. Wenn die an Ihre Amazon EC2 EC2-Instance angeschlossene Netzwerkschnittstelle beispielsweise bis zu 10 Gbit/s verarbeiten kann, werden Volumes über 10 Gbit/s langsamer und blockieren möglicherweise den Datenverkehr zu dieser Instance. Während eines Angriffs befördert Shield Advanced Ihre Netzwerk-ACL bis AWS an die Grenze, wodurch mehrere Terabyte an Datenverkehr verarbeitet werden können. Ihre Netzwerk-ACL kann Schutz für Ihre Ressource weit über die typische Kapazität Ihres Netzwerks hinaus bieten. Weitere Informationen zu Netzwerk-ACLs finden Sie unter [Network ACLs](#).

Bei einigen Skalierungstools AWS Elastic Beanstalk, z. B., können Sie einem Network Load Balancer nicht automatisch eine Elastic IP-Adresse zuordnen. In diesen Fällen müssen Sie die Elastic IP-Adresse manuell anhängen.

AWS Shield Advanced Schutzmaßnahmen auf Anwendungsebene (Schicht 7)

Um Ihre Ressourcen auf Anwendungsebene mit Shield Advanced zu schützen, verknüpfen Sie zunächst eine AWS WAF Web-ACL mit der Ressource und fügen ihr eine oder mehrere ratenbasierte Regeln hinzu. Sie können zusätzlich die automatische DDoS-Abwehr auf Anwendungsebene aktivieren, wodurch Shield Advanced als Reaktion auf DDoS-Angriffe automatisch Web-ACL-Regeln in Ihrem Namen erstellt und verwaltet.

Wenn Sie eine Ressource auf Anwendungsebene mit Shield Advanced schützen, analysiert Shield Advanced den Datenverkehr im Laufe der Zeit, um Baselines festzulegen und aufrechtzuerhalten. Shield Advanced verwendet diese Baselines, um Anomalien in den Verkehrsmustern zu erkennen, die auf einen DDoS-Angriff hinweisen könnten. Der Zeitpunkt, an dem Shield Advanced einen Angriff erkennt, hängt vom Verkehr ab, den Shield Advanced vor dem Angriff beobachten konnte, und von der Architektur, die Sie für Ihre Webanwendungen verwenden. Zu den Architekturvariationen, die das Verhalten von Shield Advanced beeinflussen können, gehören der Typ der von Ihnen verwendeten Instanz, Ihre Instanzgröße und ob der Instance-Typ Enhanced Networking unterstützt. Sie können

Shield Advanced auch so konfigurieren, dass automatisch Gegenmaßnahmen gegen Angriffe auf Anwendungsebene eingerichtet werden.

Shield Advanced-Abonnements und AWS WAF Kosten

Ihr Shield Advanced-Abonnement deckt die Kosten für die Nutzung von AWS WAF Standardfunktionen für Ressourcen ab, die Sie mit Shield Advanced schützen. Die AWS WAF Standardgebühren, die durch Ihre Shield Advanced-Schutzmaßnahmen abgedeckt werden, sind die Kosten pro Web-ACL, die Kosten pro Regel und der Grundpreis pro Million Anfragen für die Prüfung von Webanfragen, bis zu 1.500 WCUs und bis zur Standardkörpergröße.

Durch die Aktivierung der automatischen DDoS-Abwehr auf Anwendungsebene von Shield Advanced wird Ihrer Web-ACL eine Regelgruppe hinzugefügt, die 150 Web-ACL-Kapazitätseinheiten (WCUs) verwendet. Diese WCUs werden auf die WCU-Nutzung in Ihrer Web-ACL angerechnet. Weitere Informationen finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#), [Die Shield Advanced-Regelgruppe](#) und [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#).

Ihr Abonnement AWS WAF für Shield Advanced deckt nicht die Nutzung von Ressourcen ab, die Sie nicht mit Shield Advanced schützen. Es deckt auch keine zusätzlichen, nicht standardmäßigen AWS WAF Kosten für geschützte Ressourcen ab. Beispiele für nicht standardmäßige AWS WAF Kosten sind die Kosten für Bot-Kontrolle, für CAPTCHA Regelaktionen, für Web-ACLs, die mehr als 1.500 WCUs verwenden, und für die Überprüfung des Anforderungstexts, der über die Standardgröße hinausgeht. Die vollständige Liste finden Sie auf der Seite mit den Preisen. AWS WAF

Vollständige Informationen und Preisbeispiele finden Sie unter [Shield Pricing](#) and [AWS WAF Pricing](#).

Themen

- [Erkennung und Schadensbegrenzung](#)
- [Shield Advanced AWS WAF Web-ACLs und ratenbasierte Regeln auf Anwendungsebene](#)
- [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#)

Erkennung und Schadensbegrenzung

In diesem Abschnitt werden die Faktoren beschrieben, die die Erkennung und Abwehr von Ereignissen auf Anwendungsebene durch Shield Advanced beeinflussen.

Health checks (Zustandsprüfungen)

Integritätsprüfungen, die den Gesamtzustand Ihrer Anwendung genau melden, liefern Shield Advanced Informationen über die Verkehrsbedingungen, denen Ihre Anwendung ausgesetzt ist. Shield Advanced benötigt weniger Informationen, die auf einen potenziellen Angriff hinweisen, wenn Ihre Anwendung als fehlerhaft gemeldet wird, und es werden mehr Beweise für einen Angriff benötigt, wenn Ihre Anwendung als fehlerfrei gemeldet wird.

Es ist wichtig, dass Sie Ihre Integritätsprüfungen so konfigurieren, dass sie den Zustand der Anwendung korrekt melden. Weitere Informationen und Anleitungen finden Sie unter [Gesundheitsbasierte Erkennung mithilfe von Gesundheitschecks](#).

Ausgangswerte für den Verkehr

Verkehrs-Baselines geben Shield Advanced Informationen über die Eigenschaften des normalen Datenverkehrs für Ihre Anwendung. Shield Advanced verwendet diese Baselines, um zu erkennen, wenn Ihre Anwendung keinen normalen Datenverkehr empfängt. Auf diese Weise kann es Sie benachrichtigen und, wie konfiguriert, mit der Entwicklung und dem Testen von Abwehroptionen beginnen, um einem potenziellen Angriff entgegenzuwirken. Weitere Informationen darüber, wie Shield Advanced Verkehrsbaselines verwendet, um potenzielle Ereignisse zu erkennen, finden Sie im Abschnitt [Übersicht. Erkennungslogik für Bedrohungen auf Anwendungsebene](#)

Shield Advanced erstellt seine Baselines anhand von Informationen, die von der Web-ACL bereitgestellt werden, die der geschützten Ressource zugeordnet ist. Die Web-ACL muss mindestens 24 Stunden und bis zu 30 Tage mit der Ressource verknüpft sein, bevor Shield Advanced die Baselines der Anwendung zuverlässig ermitteln kann. Die benötigte Zeit beginnt, wenn Sie die Web-ACL zuordnen, entweder über Shield Advanced oder über AWS WAF.

Weitere Informationen zur Verwendung einer Web-ACL mit Ihrem Shield Advanced-Schutz auf Anwendungsebene finden Sie unter [Shield Advanced AWS WAF Web-ACLs und ratenbasierte Regeln auf Anwendungsebene](#).

Ratenbasierte Regeln

Ratenbasierte Regeln können zur Abwehr von Angriffen beitragen. Sie können Angriffe auch verschleiern, indem sie sie abwehren, bevor sie zu einem Problem werden, das groß genug ist, um in normalen Datenverkehrsdaten oder in Statusberichten zum Status von Gesundheitschecks aufzutauchen.

Wir empfehlen, ratenbasierte Regeln in Ihrer Web-ACL zu verwenden, wenn Sie eine Anwendungsressource mit Shield Advanced schützen. Auch wenn ihre Abwehr einen potenziellen

Angriff verdecken kann, stellen sie eine wertvolle erste Verteidigungslinie dar und tragen dazu bei, dass Ihre Anwendung Ihren legitimen Kunden weiterhin zur Verfügung steht. Der Traffic, den Ihre tarifbasierten Regeln erkennen, und das Ratenlimit sind in Ihren Kennzahlen sichtbar. AWS WAF

Wenn Sie die automatische DDoS-Abwehr auf Anwendungsebene aktivieren, fügt Shield Advanced Ihrer Web-ACL zusätzlich zu Ihren eigenen ratenbasierten Regeln eine Regelgruppe hinzu, die zur Abwehr von Angriffen verwendet wird. In dieser Regelgruppe verfügt Shield Advanced immer über eine ratenbasierte Regel, die das Volumen der Anfragen von IP-Adressen begrenzt, von denen bekannt ist, dass sie Quellen von DDoS-Angriffen sind. Metriken für den Verkehr, den die Shield Advanced-Regeln abschwächen, können Sie nicht einsehen.


Weitere Informationen zu ratenbasierten Regeln finden Sie unter [Ratenbasierte Regelanweisung](#). Informationen zu der ratenbasierten Regel, die Shield Advanced für die automatische DDoS-Abwehr auf Anwendungsebene verwendet, finden Sie unter [Die Shield Advanced-Regelgruppe](#).

Weitere Informationen zu Shield Advanced und AWS WAF Metriken finden Sie unter [Überwachung mit Amazon CloudWatch](#).

Shield Advanced AWS WAF Web-ACLs und ratenbasierte Regeln auf Anwendungsebene


Um eine Ressource auf Anwendungsebene mit Shield Advanced zu schützen, ordnen Sie der Ressource zunächst eine AWS WAF Web-ACL zu. AWS WAF ist eine Firewall für Webanwendungen, mit der Sie die HTTP- und HTTPS-Anfragen überwachen können, die an Ihre Ressourcen auf Anwendungsebene weitergeleitet werden, und mit der Sie den Zugriff auf Ihre Inhalte anhand der Eigenschaften der Anfragen steuern können. Sie können eine Web-ACL so konfigurieren, dass Anfragen auf der Grundlage von Faktoren wie dem Ursprung der Anfrage, dem Inhalt von Abfragezeichenfolgen und Cookies sowie der Rate der Anfragen, die von einer einzigen IP-Adresse kommen, überwacht und verwaltet werden. Für Ihren Shield Advanced-Schutz müssen Sie mindestens eine Web-ACL mit einer ratenbasierten Regel verknüpfen, die die Anzahl der Anfragen für jede IP-Adresse begrenzt.

Wenn für die zugehörige Web-ACL keine ratenbasierte Regel definiert ist, fordert Shield Advanced Sie auf, mindestens eine zu definieren. Ratenbasierte Regeln blockieren automatisch den Datenverkehr von Quell-IPs, wenn diese die von Ihnen definierten Schwellenwerte überschreiten. Sie tragen dazu bei, Ihre Anwendung vor einer Flut von Webanfragen zu schützen, und können Warnmeldungen über plötzliche Datenverkehrsspitzen ausgeben, die auf einen möglichen DDoS-Angriff hinweisen könnten.

 Note

Eine ratenbasierte Regel reagiert sehr schnell auf Datenverkehrsspitzen, die von der Regel überwacht werden. Aus diesem Grund kann eine ratenbasierte Regel nicht nur einen Angriff verhindern, sondern auch die Erkennung eines potenziellen Angriffs durch die Erkennung von Shield Advanced. Bei diesem Kompromiss wird die Prävention der vollständigen Transparenz der Angriffsmuster vorgezogen. Wir empfehlen, eine ratenbasierte Regel als erste Verteidigungslinie gegen Angriffe zu verwenden.

Wenn Ihre Web-ACL eingerichtet ist, können Sie bei einem DDoS-Angriff Gegenmaßnahmen ergreifen, indem Sie Regeln in der Web-ACL hinzufügen und verwalten. Sie können dies direkt mit Unterstützung des Shield Response Teams (SRT) oder automatisch durch automatische DDoS-Abwehr auf Anwendungsebene tun.

 Important

Wenn Sie auch die automatische DDoS-Abwehr auf Anwendungsebene verwenden, finden Sie die Best Practices für die Verwaltung Ihrer Web-ACL unter. [Bewährte Methoden für die Verwendung der automatischen Schadensbegrenzung](#)

Standardverhalten bei ratenbasierten Regeln

Wenn Sie eine ratenbasierte Regel mit ihrer Standardkonfiguration verwenden, wird in AWS WAF regelmäßigen Abständen der Verkehr für das vorherige 5-minütige Zeitfenster ausgewertet. AWS WAF blockiert Anfragen von beliebigen IP-Adressen, die den Schwellenwert der Regel überschreiten, bis die Anforderungsrate auf ein akzeptables Niveau gesunken ist. Wenn Sie eine ratenbasierte Regel über Shield Advanced konfigurieren, konfigurieren Sie deren Schwellenwert auf einen Wert, der höher ist als die normale Datenverkehrsrate, die Sie von einer beliebigen Quell-IP in einem beliebigen Zeitfenster von fünf Minuten erwarten.

Möglicherweise möchten Sie mehr als eine ratenbasierte Regel in einer Web-ACL verwenden. Sie könnten beispielsweise eine ratenbasierte Regel für den gesamten Datenverkehr mit einem hohen Schwellenwert sowie eine oder mehrere zusätzliche Regeln verwenden, die so konfiguriert sind, dass sie ausgewählten Teilen Ihrer Webanwendung entsprechen und niedrigere Schwellenwerte haben. Sie könnten beispielsweise die URI `/login.html` einem niedrigeren Schwellenwert zuordnen, um den Missbrauch einer Anmeldeseite zu verhindern.

Sie können eine ratenbasierte Regel so konfigurieren, dass sie ein anderes Bewertungszeitfenster verwendet und Anfragen nach einer Reihe von Anforderungskomponenten wie Header-Werten, Labels und Abfrageargumenten aggregiert. Weitere Informationen finden Sie unter [Ratenbasierte Regeln](#).

Weitere Informationen und Anleitungen finden Sie im Sicherheits-Blogbeitrag [Die drei wichtigsten AWS WAF ratenbasierten Regeln](#).

Erweiterte Konfigurationsoptionen durch AWS WAF

Die Shield Advanced-Konsole ermöglicht es Ihnen, eine ratenbasierte Regel hinzuzufügen und sie mit den grundlegenden Standardeinstellungen zu konfigurieren. Sie können zusätzliche Konfigurationsoptionen definieren, indem Sie Ihre ratenbasierten Regeln über [Verwalten](#) verwalten. AWS WAF Sie können die Regel beispielsweise so konfigurieren, dass Anfragen auf der Grundlage von Schlüsseln wie einer weitergeleiteten IP-Adresse, einer Abfragezeichenfolge und einer Bezeichnung zusammengefasst werden. Sie können der Regel auch eine Scopedown-Anweisung hinzufügen, um einige Anfragen aus der Bewertung und der Ratenbegrenzung herauszufiltern. Weitere Informationen finden Sie unter [Ratenbasierte Regeln](#). Informationen AWS WAF zur Verwaltung Ihrer Überwachungs- und Verwaltungsregeln für Webanfragen finden Sie unter [Erstellen einer Web-ACL](#).

Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene

Sie können Shield Advanced so konfigurieren, dass es automatisch reagiert, um Angriffe auf Anwendungsebene (Schicht 7) gegen Ihre geschützten Ressourcen auf Anwendungsebene abzuwehren, indem Webanfragen, die Teil des Angriffs sind, gezählt oder blockiert werden. Diese Option ist eine Ergänzung zum Schutz auf Anwendungsebene, den Sie über Shield Advanced mit einer AWS WAF Web-ACL und Ihrer eigenen ratenbasierten Regel hinzufügen.

Wenn die automatische Risikominderung für eine Ressource aktiviert ist, verwaltet Shield Advanced eine Regelgruppe in der zugehörigen Web-ACL der Ressource, in der es Minderungsregeln im Namen der Ressource verwaltet. Die Regelgruppe enthält eine ratenbasierte Regel, die das Volumen der Anfragen von IP-Adressen verfolgt, von denen bekannt ist, dass sie Quellen von DDoS-Angriffen sind.

Darüber hinaus vergleicht Shield Advanced aktuelle Verkehrsmuster mit historischen Verkehrsbasislinien, um Abweichungen zu erkennen, die auf einen DDoS-Angriff hinweisen könnten. Shield Advanced reagiert auf erkannte DDoS-Angriffe, indem es zusätzliche benutzerdefinierte AWS WAF Regeln in der Regelgruppe erstellt, auswertet und einsetzt.

Inhalt

- [Vorbehalte bei der Verwendung der automatischen Schadensbegrenzung](#)
- [Bewährte Methoden für die Verwendung der automatischen Schadensbegrenzung](#)
- [Konfiguration erforderlich, um die automatische Risikominderung zu aktivieren](#)
- [So verwaltet Shield Advanced die automatische Schadensbegrenzung](#)
 - [Was passiert, wenn Sie die automatische Abwehr aktivieren](#)
 - [Wie Shield Advanced mit automatischer Abwehr auf DDoS-Angriffe reagiert](#)
 - [So verwaltet Shield Advanced die Einstellung für Regelaktionen](#)
 - [So verwaltet Shield Advanced Abhilfemaßnahmen, wenn ein Angriff nachlässt](#)
 - [Was passiert, wenn Sie die automatische Abwehr deaktivieren](#)
- [Die Shield Advanced-Regelgruppe](#)
- [Verwaltung der automatischen DDoS-Abwehr auf Anwendungsebene](#)
 - [Konfiguration zur automatischen DDoS-Abwehr auf Anwendungsebene für eine Ressource anzeigen](#)
 - [Automatische DDoS-Abwehr auf Anwendungsebene aktivieren und deaktivieren](#)
 - [Änderung der Aktion, die für die automatische DDoS-Abwehr auf Anwendungsebene verwendet wird](#)
 - [Verwendung AWS CloudFormation mit automatischer DDoS-Abwehr auf Anwendungsebene](#)

Vorbehalte bei der Verwendung der automatischen Schadensbegrenzung

In der folgenden Liste werden die Vorbehalte der automatischen DDoS-Abwehr auf Anwendungsebene von Shield Advanced beschrieben und die Schritte beschrieben, die Sie möglicherweise als Reaktion darauf ergreifen sollten.

- Die automatische DDoS-Abwehr auf Anwendungsebene funktioniert nur mit Web-ACLs, die mit der neuesten Version von (v2) erstellt wurden. AWS WAF
- Shield Advanced benötigt Zeit, um eine Basislinie des normalen, historischen Datenverkehrs Ihrer Anwendung zu erstellen, die es nutzt, um den Angriffsverkehr zu erkennen und vom normalen Verkehr zu isolieren, um den Angriffsverkehr einzudämmen. Die Erstellung einer Baseline dauert zwischen 24 Stunden und 30 Tagen ab dem Zeitpunkt, an dem Sie der geschützten Anwendungsressource eine Web-ACL zuordnen. Weitere Informationen zu Verkehrs-Baselines finden Sie unter [Erkennung und Schadensbegrenzung](#)
- Wenn Sie die automatische DDoS-Abwehr auf Anwendungsebene aktivieren, wird Ihrer Web-ACL eine Regelgruppe hinzugefügt, die 150 Web-ACL-Kapazitätseinheiten (WCUs) verwendet.

Diese WCUs werden auf die WCU-Nutzung in Ihrer Web-ACL angerechnet. Weitere Informationen finden Sie unter [Die Shield Advanced-Regelgruppe](#) und [AWS WAF Web-ACL-Kapazitätseinheiten \(WCUs\)](#).

- Die Shield Advanced-Regelgruppe generiert AWS WAF Metriken, die jedoch nicht angezeigt werden können. Das Gleiche gilt für alle anderen Regelgruppen, die Sie in Ihrer Web-ACL verwenden, die Sie aber nicht besitzen, wie z. B. Regelgruppen mit AWS verwalteten Regeln. Weitere Informationen zu AWS WAF Metriken finden Sie unter [AWS WAF Metriken und Dimensionen](#). Informationen zu dieser Shield Advanced-Schutzoption finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#).
- Bei Web-ACLs, die mehrere Ressourcen schützen, werden bei der automatischen Risikominderung nur benutzerdefinierte Abhilfemaßnahmen eingesetzt, die sich auf keine der geschützten Ressourcen negativ auswirken.
- Die Zeit zwischen dem Beginn eines DDoS-Angriffs und dem Zeitpunkt, zu dem Shield Advanced benutzerdefinierte Regeln zur automatischen Abwehr festlegt, ist von Ereignis zu Ereignis unterschiedlich. Einige DDoS-Angriffe können enden, bevor die benutzerdefinierten Regeln implementiert werden. Andere Angriffe können auftreten, wenn bereits eine Abwehr vorhanden ist, sodass diese von Beginn des Ereignisses an durch diese Regeln abgewehrt werden können. Darüber hinaus können ratenbasierte Regeln in der Web-ACL- und Shield-Advanced-Regelgruppe den Angriffsverkehr abschwächen, bevor er als mögliches Ereignis erkannt wird.
- Für Application Load Balancer, die jeglichen Datenverkehr über ein Content Delivery Network (CDN) empfangen, wie Amazon CloudFront, werden die automatischen Abwehrfunktionen von Shield Advanced auf Anwendungsebene für diese Application Load Balancer-Ressourcen reduziert. Shield Advanced verwendet Client-Datenverkehrsattribute, um den Angriffsverkehr zu identifizieren und vom normalen Datenverkehr an Ihre Anwendung zu isolieren. CDNs behalten oder leiten die ursprünglichen Client-Traffic-Attribute möglicherweise nicht weiter. Wenn Sie dies verwenden CloudFront, empfehlen wir, die automatische Abwehr für die CloudFront Verteilung zu aktivieren.
- Die automatische DDoS-Abwehr auf Anwendungsebene interagiert nicht mit Schutzgruppen. Sie können die automatische Abwehr für Ressourcen aktivieren, die sich in Schutzgruppen befinden, aber Shield Advanced wendet nicht automatisch Angriffsabwehrmaßnahmen an, die auf den Ergebnissen der Schutzgruppe basieren. Shield Advanced wendet automatische Angriffsabwehrmaßnahmen für einzelne Ressourcen an.

Bewährte Methoden für die Verwendung der automatischen Schadensbegrenzung

Halten Sie sich bei der Verwendung der automatischen Abwehr an die Anweisungen in diesem Abschnitt.

Verwaltung allgemeiner Schutzmaßnahmen

Halten Sie sich bei der Planung und Implementierung Ihrer automatischen Schutzmaßnahmen an diese Richtlinien.

- Verwalten Sie Ihren gesamten automatischen Schadensbegrenzungsschutz entweder über Shield Advanced oder, falls Sie Ihre Einstellungen AWS Firewall Manager zur automatischen Abwehr von Shield Advanced verwenden, über Firewall Manager. Verwenden Sie Shield Advanced und Firewall Manager nicht gleichzeitig, um diese Schutzmaßnahmen zu verwalten.
- Verwalten Sie ähnliche Ressourcen mit denselben Web-ACLs und Schutzeinstellungen und verwalten Sie unterschiedliche Ressourcen mit unterschiedlichen Web-ACLs. Wenn Shield Advanced einen DDoS-Angriff auf eine geschützte Ressource abwehrt, definiert es Regeln für die Web-ACL, die der Ressource zugeordnet ist, und testet dann die Regeln anhand des Datenverkehrs aller Ressourcen, die mit der Web-ACL verknüpft sind. Shield Advanced wendet die Regeln nur an, wenn sie sich nicht negativ auf die zugehörigen Ressourcen auswirken. Weitere Informationen finden Sie unter [So verwaltet Shield Advanced die automatische Schadensbegrenzung](#).
- Aktivieren Sie für Application Load Balancer, deren gesamter Internetverkehr über eine CloudFront Amazon-Distribution weitergeleitet wird, nur die automatische Schadensbegrenzung für die Verteilung. CloudFront Die CloudFront Distribution wird immer über die größte Anzahl an ursprünglichen Datenverkehrsattributen verfügen, die Shield Advanced zur Abwehr von Angriffen nutzt.

Optimierung der Erkennung und Abwehr

Folgen Sie diesen Richtlinien, um den Schutz zu optimieren, den die automatische Schadensbegrenzung für geschützte Ressourcen bietet. Einen Überblick über die Erkennung und Abwehr auf Anwendungsebene finden Sie unter [Erkennung und Schadensbegrenzung](#)

- Konfigurieren Sie Integritätsprüfungen für Ihre geschützten Ressourcen und verwenden Sie sie, um eine gesundheitsbasierte Erkennung in Ihren Shield Advanced-Schutzmaßnahmen zu ermöglichen. Anleitungen finden Sie unter [Gesundheitsbasierte Erkennung mithilfe von Gesundheitschecks](#).

- Aktivieren Sie die automatische Schadensbegrenzung im Count Modus, bis Shield Advanced eine Ausgangsbasis für normalen, historischen Datenverkehr festgelegt hat. Shield Advanced benötigt zwischen 24 Stunden und 30 Tagen, um einen Basiswert festzulegen.

Um eine Basislinie für normale Verkehrsmuster zu erstellen, ist Folgendes erforderlich:

- Die Zuordnung einer Web-ACL zur geschützten Ressource. Sie können sie AWS WAF direkt verwenden, um Ihre Web-ACL zuzuordnen, oder Sie können sie von Shield Advanced zuordnen lassen, wenn Sie den Shield Advanced-Schutz auf Anwendungsebene aktivieren und eine zu verwendende Web-ACL angeben.
- Normaler Datenfluss zu Ihrer geschützten Anwendung. Wenn bei Ihrer Anwendung kein normaler Datenverkehr stattfindet, z. B. bevor die Anwendung gestartet wird, oder wenn es für längere Zeit zu wenig Produktionsdatenverkehr gibt, können die historischen Daten nicht erfasst werden.

Verwaltung von Web-ACLs

Folgen Sie diesen Richtlinien für die Verwaltung der Web-ACLs, die Sie mit automatischer Risikominderung verwenden.

- Wenn Sie die Web-ACL ersetzen müssen, die der geschützten Ressource zugeordnet ist, nehmen Sie die folgenden Änderungen der Reihe nach vor:
 1. Deaktivieren Sie in Shield Advanced die automatische Schadensbegrenzung.
 2. AWS WAF Trennen Sie in die alte Web-ACL und ordnen Sie die neue Web-ACL zu.
 3. Aktivieren Sie in Shield Advanced die automatische Schadensbegrenzung.

Shield Advanced überträgt die automatische Abwehr nicht automatisch von der alten Web-ACL auf die neue.

- Löschen Sie keine Regelgruppenregel aus Ihren Web-ACLs, deren Name mit `ShieldMitigationRuleGroup` beginnt. Wenn Sie diese Regelgruppe löschen, deaktivieren Sie den Schutz, der durch die automatische Schadensbegrenzung von Shield Advanced für jede Ressource bereitgestellt wird, die mit der Web-ACL verknüpft ist. Darüber hinaus kann es einige Zeit dauern, bis Shield Advanced eine Benachrichtigung über die Änderung erhält und die Einstellungen aktualisiert. Während dieser Zeit werden auf den Seiten der Shield Advanced-Konsole falsche Informationen angezeigt.

Weitere Informationen zur Regelgruppe finden Sie unter [Die Shield Advanced-Regelgruppe](#).

- Ändern Sie nicht den Namen einer Regelgruppenregel, deren Name mit `ShieldMitigationRuleGroup` beginnt. Dies kann die Schutzmaßnahmen beeinträchtigen, die durch die automatische Abwehr von Shield Advanced über die Web-ACL bereitgestellt werden.
- Verwenden Sie beim Erstellen von Regeln und Regelgruppen keine Namen, die mit `ShieldMitigationRuleGroup` beginnen. Diese Zeichenfolge wird von Shield Advanced verwendet, um Ihre automatischen Gegenmaßnahmen zu verwalten.
- Weisen Sie bei der Verwaltung Ihrer Web-ACL-Regeln keine Prioritätseinstellung von 10.000.000 zu. Shield Advanced weist diese Prioritätseinstellung seiner Gruppenregel für automatische Schadensbegrenzung zu, wenn es sie hinzufügt.
- Sorgen Sie dafür, dass die `ShieldMitigationRuleGroup` Regel im Verhältnis zu den anderen Regeln in Ihrer Web-ACL zu dem von Ihnen gewünschten Zeitpunkt ausgeführt wird. Shield Advanced fügt der Web-ACL die Regelgruppenregel mit der Priorität 10.000.000 hinzu, sodass sie nach Ihren anderen Regeln ausgeführt wird. Wenn Sie den AWS WAF Konsolenassistenten zur Verwaltung Ihrer Web-ACL verwenden, passen Sie die Prioritätseinstellungen nach dem Hinzufügen von Regeln zur Web-ACL nach Bedarf an.
- Wenn Sie Ihre Web-ACLs AWS CloudFormation zur Verwaltung verwenden, müssen Sie die `ShieldMitigationRuleGroup` Regelgruppenregel nicht verwalten. Folgen Sie den Anweisungen unter [Verwendung AWS CloudFormation mit automatischer DDoS-Abwehr auf Anwendungsebene](#)

Konfiguration erforderlich, um die automatische Risikominderung zu aktivieren

Sie aktivieren die automatische Abwehr von Shield Advanced als Teil des DDoS-Schutzes auf Anwendungsebene für Ihre Ressource. Informationen dazu, wie Sie dies über die Konsole tun können, finden Sie unter [Konfigurieren Sie den DDoS-Schutz auf Anwendungsebene](#)

Für die automatische Schadensbegrenzungsfunktion müssen Sie wie folgt vorgehen:

- Ordnen Sie der Ressource eine Web-ACL zu — Dies ist für jeden Shield Advanced-Schutz auf Anwendungsebene erforderlich. Sie können dieselbe Web-ACL für mehrere Ressourcen verwenden. Wir empfehlen, dies nur für Ressourcen mit ähnlichem Datenverkehr zu tun. Informationen zu Web-ACLs, einschließlich der Anforderungen für deren Verwendung mit mehreren Ressourcen, finden Sie unter [Wie AWS WAF funktioniert](#).
- Automatische DDoS-Abwehr auf Anwendungsebene von Shield Advanced aktivieren und konfigurieren — Wenn Sie diese Option aktivieren, geben Sie an, ob Shield Advanced Webanfragen, die als Teil eines DDoS-Angriffs eingestuft werden, automatisch blockieren oder

zählen soll. Shield Advanced fügt der zugehörigen Web-ACL eine Regelgruppe hinzu und verwendet sie, um ihre Reaktion auf DDoS-Angriffe auf die Ressource dynamisch zu verwalten. Informationen zu den Aktionsoptionen für Regeln finden Sie unter [Regelaktion](#).

- (Optional, aber empfohlen) Fügen Sie der Web-ACL eine ratenbasierte Regel hinzu — Standardmäßig bietet die ratenbasierte Regel Ihrer Ressource grundlegenden Schutz vor DDoS-Angriffen, indem sie verhindert, dass eine einzelne IP-Adresse in kurzer Zeit zu viele Anfragen sendet. Informationen zu ratenbasierten Regeln, einschließlich Optionen für die Aggregation benutzerdefinierter Anfragen und Beispiele, finden Sie unter [Ratenbasierte Regelanweisung](#)

So verwaltet Shield Advanced die automatische Schadensbegrenzung

In den Abschnitten wird beschrieben, wie Shield Advanced mit Ihren Konfigurationsänderungen für die automatische DDoS-Abwehr auf Anwendungsebene umgeht und wie es mit DDoS-Angriffen umgeht, wenn die automatische Abwehr aktiviert ist.

Themen

- [Was passiert, wenn Sie die automatische Abwehr aktivieren](#)
- [Wie Shield Advanced mit automatischer Abwehr auf DDoS-Angriffe reagiert](#)
- [So verwaltet Shield Advanced die Einstellung für Regelaktionen](#)
- [So verwaltet Shield Advanced Abhilfemaßnahmen, wenn ein Angriff nachlässt](#)
- [Was passiert, wenn Sie die automatische Abwehr deaktivieren](#)

Was passiert, wenn Sie die automatische Abwehr aktivieren

Shield Advanced macht Folgendes, wenn Sie die automatische Schadensbegrenzung aktivieren:

- Fügt bei Bedarf eine Regelgruppe für die Verwendung von Shield Advanced hinzu — Wenn die AWS WAF Web-ACL, die Sie der Ressource zugeordnet haben, nicht bereits über eine AWS WAF Regelgruppenregel verfügt, die der automatischen DDoS-Abwehr auf Anwendungsebene gewidmet ist, fügt Shield Advanced eine hinzu.

Der Name der Regelgruppenregel beginnt mit `ShieldMitigationRuleGroup`

Die Regelgruppe enthält immer eine ratenbasierte Regel mit dem

Namen `ShieldKnownOffenderIPRateBasedRule`, die das Volumen der Anfragen von IP-Adressen begrenzt, von denen bekannt ist, dass sie Quellen von DDoS-Angriffen sind. Weitere Informationen zur Shield Advanced-Regelgruppe und der Web-ACL-Regel, die auf sie verweist, finden Sie unter [Die Shield Advanced-Regelgruppe](#).

- Beginnt, auf DDoS-Angriffe gegen die Ressource zu reagieren — Shield Advanced reagiert automatisch auf DDoS-Angriffe für die geschützte Ressource. Zusätzlich zur ratenbasierten Regel, die immer vorhanden ist, verwendet Shield Advanced seine Regelgruppe, um benutzerdefinierte AWS WAF Regeln zur Abwehr von DDoS-Angriffen bereitzustellen. Shield Advanced passt diese Regeln an Ihre Anwendung und die Angriffe an, denen Ihre Anwendung ausgesetzt ist, und testet sie vor der Bereitstellung anhand des historischen Datenverkehrs der Ressource.

Shield Advanced verwendet eine einzige Regelgruppenregel in jeder Web-ACL, die Sie für die automatische Schadensbegrenzung verwenden. Wenn Shield Advanced die Regelgruppe für eine andere geschützte Ressource bereits hinzugefügt hat, fügt es der Web-ACL keine weitere Regelgruppe hinzu.

Die automatische Abwehr von DDoS-Angriffen auf Anwendungsebene hängt vom Vorhandensein der Regelgruppe ab. Wenn die Regelgruppe aus irgendeinem Grund aus der AWS WAF Web-ACL entfernt wird, deaktiviert das Entfernen die automatische Abwehr für alle Ressourcen, die der Web-ACL zugeordnet sind.

Wie Shield Advanced mit automatischer Abwehr auf DDoS-Angriffe reagiert

Wenn Sie die automatische Abwehr für eine geschützte Ressource aktiviert haben, reagiert die ratenbasierte Regel `ShieldKnownOffenderIPRateBasedRule` in der Shield Advanced-Regelgruppe automatisch auf erhöhte Datenverkehrsmengen aus bekannten DDoS-Quellen. Diese Ratenbegrenzung wird schnell angewendet und dient als Schutz an vorderster Front gegen Angriffe.

Wenn Shield Advanced einen Angriff erkennt, geht es wie folgt vor:

1. Versucht, eine Angriffssignatur zu identifizieren, die den Angriffsverkehr vom normalen Datenverkehr zu Ihrer Anwendung isoliert. Ziel ist es, hochwertige Regeln zur DDoS-Abwehr zu erstellen, die, wenn sie eingeführt werden, nur den Angriffsverkehr betreffen und den normalen Datenverkehr zu Ihrer Anwendung nicht beeinträchtigen.
2. Vergleicht die identifizierte Angriffssignatur anhand der historischen Datenverkehrsmuster für die angegriffene Ressource sowie für alle anderen Ressourcen, die derselben Web-ACL zugeordnet sind. Shield Advanced tut dies, bevor es irgendwelche Regeln als Reaktion auf das Ereignis einsetzt.

Abhängig von den Evaluierungsergebnissen führt Shield Advanced eine der folgenden Aktionen aus:

- Wenn Shield Advanced feststellt, dass die Angriffssignatur nur den Datenverkehr isoliert, der an dem DDoS-Angriff beteiligt ist, implementiert Shield Advanced die Signatur in AWS WAF Regeln in der Regelgruppe Shield Advanced-Mitigation in der Web-ACL. Shield Advanced gibt diesen Regeln die Aktionseinstellung, die Sie für die automatische Risikominderung der Ressource konfiguriert haben — entweder Count oder Block.
- Andernfalls führt Shield Advanced keine Abschwächung durch.

Während eines Angriffs sendet Shield Advanced dieselben Benachrichtigungen und stellt dieselben Ereignisinformationen bereit wie für grundlegende Shield Advanced-Schutzmaßnahmen auf Anwendungsebene. Sie können die Informationen über Ereignisse und DDoS-Angriffe sowie über alle Shield Advanced-Abhilfemaßnahmen für Angriffe in der Shield Advanced-Ereigniskonsole einsehen. Weitere Informationen finden Sie unter [Einblick in DDoS-Ereignisse](#).

Wenn Sie die automatische Schadensbegrenzung so konfiguriert haben, dass sie die Block Regelaktion verwendet, und Sie aufgrund der von Shield Advanced bereitgestellten Risikominderungsregeln Fehlalarme erhalten, können Sie die Regelaktion ändern. Count Informationen dazu finden Sie unter [Änderung der Aktion, die für die automatische DDoS-Abwehr auf Anwendungsebene verwendet wird](#)

So verwaltet Shield Advanced die Einstellung für Regelaktionen

Sie können die Regelaktion für Ihre automatischen Abhilfemaßnahmen auf Block oder festlegen. Count

Wenn Sie die Aktionseinstellung der automatischen Schadensbegrenzungsregel für eine geschützte Ressource ändern, aktualisiert Shield Advanced alle Regeleinstellungen für die Ressource. Es aktualisiert alle Regeln, die derzeit für die Ressource in der Shield Advanced-Regelgruppe gelten, und verwendet die neue Aktionseinstellung, wenn es neue Regeln erstellt.

Wenn Sie für Ressourcen, die dieselbe Web-ACL verwenden, unterschiedliche Aktionen angeben, verwendet Shield Advanced die Block Aktionseinstellung für die ratenbasierte Regel der Regelgruppe. `ShieldKnownOffenderIPRateBasedRule` Shield Advanced erstellt und verwaltet andere Regeln in der Regelgruppe im Namen einer bestimmten geschützten Ressource und verwendet die Aktionseinstellung, die Sie für die Ressource angegeben haben. Alle Regeln in der Shield Advanced-Regelgruppe in einer Web-ACL werden auf den Webverkehr aller zugehörigen Ressourcen angewendet.

Es kann einige Sekunden dauern, bis die Änderung der Aktionseinstellung wirksam wird. Während dieser Zeit werden Sie möglicherweise an einigen Stellen, an denen die Regelgruppe verwendet wird, die alte Einstellung und an anderen Stellen die neue Einstellung sehen.

Sie können die Einstellung für die Regelaktion für Ihre automatische Schadensbegrenzungskonfiguration auf der Ereignisseite der Konsole und auf der Konfigurationsseite der Anwendungsebene ändern. Informationen zur Seite „Ereignisse“ finden Sie unter [Reagieren auf DDoS-Ereignisse](#). Informationen zur Konfigurationsseite finden Sie unter [Konfigurieren Sie den DDoS-Schutz auf Anwendungsebene](#).

So verwaltet Shield Advanced Abhilfemaßnahmen, wenn ein Angriff nachlässt

Wenn Shield Advanced feststellt, dass Minderungsregeln, die für einen bestimmten Angriff eingesetzt wurden, nicht mehr benötigt werden, werden sie aus der Shield Advanced-Regelgruppe zur Schadensbegrenzung entfernt.

Das Entfernen von Regeln zur Schadensbegrenzung wird nicht unbedingt mit dem Ende eines Angriffs zusammenfallen. Shield Advanced überwacht Angriffsmuster, die es auf Ihren geschützten Ressourcen erkennt. Es kann sich proaktiv gegen die Wiederholung eines Angriffs mit einer bestimmten Signatur schützen, indem es die Regeln beibehält, die es gegen das erste Auftreten dieses Angriffs angewendet hat. Bei Bedarf verlängert Shield Advanced das Zeitfenster, in dem die Regeln eingehalten werden. Auf diese Weise kann Shield Advanced wiederholte Angriffe mit einer bestimmten Signatur abwehren, bevor sie sich auf Ihre geschützten Ressourcen auswirken.

Shield Advanced entfernt niemals die ratenbasierte Regel `ShieldKnownOffenderIPRateBasedRule`, die das Volumen der Anfragen von IP-Adressen begrenzt, von denen bekannt ist, dass sie Quellen von DDoS-Angriffen sind.

Was passiert, wenn Sie die automatische Abwehr deaktivieren

Shield Advanced macht Folgendes, wenn Sie die automatische Schadensbegrenzung für eine Ressource deaktivieren:

- Reagiert nicht mehr automatisch auf DDoS-Angriffe — Shield Advanced stellt seine automatischen Reaktionsaktivitäten für die Ressource ein.
- Entfernt nicht benötigte Regeln aus der Shield Advanced-Regelgruppe — Wenn Shield Advanced Regeln in seiner verwalteten Regelgruppe im Namen der geschützten Ressource verwaltet, werden sie entfernt.
- Entfernt die Shield Advanced-Regelgruppe, wenn sie nicht mehr verwendet wird — Wenn die Web-ACL, die Sie der Ressource zugeordnet haben, keiner anderen Ressource zugeordnet ist, für die

automatische Schadensbegrenzung aktiviert ist, entfernt Shield Advanced ihre Regelgruppenregel aus der Web-ACL.

Die Shield Advanced-Regelgruppe

Shield Advanced verwaltet automatische Minderungsaktivitäten mithilfe von Regeln in einer Regelgruppe, die es besitzt und für Sie verwaltet. Shield Advanced verweist auf die Regelgruppe mit einer Regel in der Web-ACL, die Sie mit Ihrer geschützten Ressource verknüpft haben.

Die Regelgruppenregel in Ihrer Web-ACL

Die Shield Advanced-Regelgruppenregel in Ihrer Web-ACL hat die folgenden Eigenschaften:

- Name (Name – `ShieldMitigationRuleGroup_`*account-id_web-acl-id_unique-identifizier*)
- Web-ACL-Kapazitätseinheiten (WCU) — 150. Diese WCUs werden auf die WCU-Nutzung in Ihrer Web-ACL angerechnet.

Shield Advanced erstellt diese Regel in Ihrer Web-ACL mit einer Prioritätseinstellung von 10.000.000, sodass sie nach Ihren anderen Regeln und Regelgruppen in der Web-ACL ausgeführt wird. AWS WAF führt die Regeln in einer Web-ACL ab der Einstellung mit der niedrigsten numerischen Priorität aus. Während der Verwaltung der Web-ACL kann sich diese Prioritätseinstellung ändern.

Die automatische Schadensbegrenzungsfunktion verbraucht keine zusätzlichen AWS WAF Ressourcen in Ihrem Konto, mit Ausnahme der WCUs, die von der Regelgruppe in Ihrer Web-ACL verwendet werden. Beispielsweise wird die Shield Advanced-Regelgruppe nicht zu den Regelgruppen Ihres Kontos gezählt. Informationen zu Kontolimits in AWS WAF finden Sie unter [AWS WAF Kontingente](#).

Regeln in der Regelgruppe

Innerhalb der referenzierten Shield Advanced-Regelgruppe unterhält Shield Advanced eine ratenbasierte Regel `ShieldKnownOffenderIPRateBasedRule`, die das Volumen der Anfragen von IP-Adressen begrenzt, von denen bekannt ist, dass sie Quellen von DDoS-Angriffen sind. Diese Regel dient als erste Verteidigungslinie gegen Angriffe, da sie in der Regelgruppe immer präsent ist und sich nicht auf die Analyse von Datenverkehrsmustern stützt, um Angriffe einzudämmen. Die Aktion dieser Regel ist wie bei den anderen Regeln in der Regelgruppe auf die Aktion festgelegt, die Sie für Ihre automatischen Abhilfemaßnahmen auswählen. Weitere Informationen über ratenbasierte Regeln finden Sie unter [Ratenbasierte Regelnweisung](#).

Note

Die ratenbasierte Regel `ShieldKnownOffenderIPRateBasedRule` funktioniert unabhängig von der Shield Advanced-Ereigniserkennung. Die automatische Abwehr ist zwar aktiviert, diese Regelrate begrenzt jedoch IP-Adressen, die bekanntermaßen Quellen von DDoS-Angriffen sind. Bei diesen IP-Adressen kann die Ratenbegrenzung der Regel Angriffe verhindern und auch verhindern, dass Angriffe in den Erkennungsinformationen von Shield Advanced erscheinen. Bei diesem Kompromiss wird die Prävention der vollständigen Transparenz der Angriffsmuster vorgezogen.

Zusätzlich zu der oben beschriebenen permanenten ratenbasierten Regel enthält die Regelgruppe alle Regeln, die Shield Advanced derzeit zur Abwehr von DDoS-Angriffen verwendet. Shield Advanced fügt diese Regeln nach Bedarf hinzu, ändert und entfernt sie. Weitere Informationen finden Sie unter [So verwaltet Shield Advanced die automatische Schadensbegrenzung](#).

Metriken

Die Regelgruppe generiert AWS WAF Metriken, aber da diese Regelgruppe Shield Advanced gehört, können diese Metriken nicht angezeigt werden. Weitere Informationen finden Sie unter [AWS WAF Metriken und Dimensionen](#).

Verwaltung der automatischen DDoS-Abwehr auf Anwendungsebene

Verwenden Sie die Anleitungen in diesem Abschnitt, um Ihre automatischen DDoS-Abwehrkonfigurationen auf Anwendungsebene zu verwalten. Informationen zur Funktionsweise der automatischen Abwehr finden Sie in den vorherigen Themen.

Note

Folgen Sie den unter beschriebenen bewährten Methoden. [Bewährte Methoden für die Verwendung der automatischen Schadensbegrenzung](#)

Themen

- [Konfiguration zur automatischen DDoS-Abwehr auf Anwendungsebene für eine Ressource anzeigen](#)
- [Automatische DDoS-Abwehr auf Anwendungsebene aktivieren und deaktivieren](#)

- [Änderung der Aktion, die für die automatische DDoS-Abwehr auf Anwendungsebene verwendet wird](#)
- [Verwendung AWS CloudFormation mit automatischer DDoS-Abwehr auf Anwendungsebene](#)

Konfiguration zur automatischen DDoS-Abwehr auf Anwendungsebene für eine Ressource anzeigen

Sie können die Konfiguration der automatischen DDoS-Abwehr auf Anwendungsebene für eine Ressource auf der Seite Geschützte Ressourcen und auf den einzelnen Schutzseiten einsehen.

Um die Konfiguration der automatischen DDoS-Abwehr auf Anwendungsebene anzuzeigen

1. Melden Sie sich bei der AWS WAF & Shield-Konsole an AWS Management Console und öffnen Sie sie unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im AWS Shield Navigationsbereich die Option Geschützte Ressourcen aus. In der Liste der geschützten Ressourcen gibt die Spalte Automatische DDoS-Abwehr auf Anwendungsebene an, ob die automatische Abwehr aktiviert ist und, sofern aktiviert, welche Aktion Shield Advanced für seine Abwehr verwenden soll.

Sie können auch eine beliebige Ressource auf Anwendungsebene auswählen, um dieselben Informationen auf der Schutzseite für die Ressource zu sehen.

Automatische DDoS-Abwehr auf Anwendungsebene aktivieren und deaktivieren

Das folgende Verfahren zeigt, wie Sie die automatische Antwort für eine geschützte Ressource aktivieren oder deaktivieren.

Um die automatische DDoS-Abwehr auf Anwendungsebene für eine einzelne Ressource zu aktivieren oder zu deaktivieren

1. Melden Sie sich bei der AWS WAF & Shield-Konsole an AWS Management Console und öffnen Sie sie unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im AWS Shield Navigationsbereich die Option Geschützte Ressourcen aus.
3. Wählen Sie auf der Registerkarte Schutz die Ressource auf Anwendungsebene aus, für die Sie die automatische Schadensbegrenzung aktivieren möchten. Die Seite mit den Schutzmaßnahmen für die Ressource wird geöffnet.
4. Wählen Sie auf der Schutzseite der Ressource die Option Bearbeiten aus.

5. Wählen Sie auf der Seite Layer-7-DDoS-Abwehr für globale Ressourcen konfigurieren — optional für Automatische DDoS-Abwehr auf Anwendungsebene die Option aus, die Sie für automatische Abwehr verwenden möchten. In der Konsole stehen die folgenden Optionen zur Verfügung:
 - Aktuelle Einstellungen beibehalten — Nehmen Sie keine Änderungen an den Einstellungen für die automatische Schadensbegrenzung der geschützten Ressource vor.
 - Aktivieren — Aktiviert die automatische Schadensbegrenzung für die geschützte Ressource. Wenn Sie diese Option wählen, wählen Sie in den Web-ACL-Regeln auch die Regelaktion aus, die von den automatischen Risikominderungen verwendet werden soll. Weitere Informationen zu Einstellungen für Regelaktionen finden Sie unter [Regelaktion](#).

Wenn Ihre geschützte Ressource noch keinen Verlauf des normalen Anwendungsverkehrs hat, aktivieren Sie die automatische Schadensbegrenzung im Count Modus, bis Shield Advanced einen Basiswert festlegen kann. Shield Advanced beginnt mit der Erfassung von Informationen für seine Baseline, wenn Sie Ihrer geschützten Ressource eine Web-ACL zuordnen. Es kann 24 Stunden bis 30 Tage dauern, bis eine gute Ausgangsbasis für normalen Datenverkehr erstellt ist.

 - Deaktivieren — Deaktiviert die automatische Schadensbegrenzung für die geschützte Ressource.
6. Gehen Sie die restlichen Seiten durch, bis Sie fertig sind, und speichern Sie die Konfiguration.

Auf der Seite Schutzmaßnahmen werden die Einstellungen für die automatische Schadensbegrenzung für die Ressource aktualisiert.

Änderung der Aktion, die für die automatische DDoS-Abwehr auf Anwendungsebene verwendet wird

Sie können die Aktion, die Shield Advanced für seine automatische Antwort auf Anwendungsebene verwendet, an mehreren Stellen in der Konsole ändern:

- Konfiguration der automatischen Schadensbegrenzung — Ändern Sie die Aktion, wenn Sie die automatische Schadensbegrenzung für Ihre Ressource konfigurieren. Das Verfahren finden Sie im vorherigen Abschnitt. [Automatische DDoS-Abwehr auf Anwendungsebene aktivieren und deaktivieren](#)
- Seite mit den Ereignisdetails — Ändern Sie die Aktion auf der Seite mit den Ereignisdetails, wenn Sie die Ereignisinformationen in der Konsole anzeigen. Weitere Informationen finden Sie unter [AWS Shield Advanced Einzelheiten zur Veranstaltung](#).

Wenn Sie über zwei geschützte Ressourcen verfügen, die sich eine Web-ACL teilen, und Sie die Aktion für die eine und Count Block für die andere auf setzen, legt Shield Advanced die Aktion für die ratenbasierte Regel `ShieldKnownOffenderIPRateBasedRule` der Regelgruppe auf fest. Block

Verwendung AWS CloudFormation mit automatischer DDoS-Abwehr auf Anwendungsebene

Erfahren Sie, wie Sie AWS CloudFormation Ihre Schutzmaßnahmen und Web-ACLs verwalten können. AWS WAF

Automatische DDoS-Abwehr auf Anwendungsebene aktivieren oder deaktivieren

Sie können die automatische DDoS-Abwehr auf Anwendungsebene mithilfe AWS CloudFormation der Ressource aktivieren und deaktivieren. `AWS::Shield::Protection` Der Effekt ist derselbe wie bei der Aktivierung oder Deaktivierung der Funktion über die Konsole oder eine andere Schnittstelle. Informationen zu der AWS CloudFormation Ressource finden Sie [AWS::Shield::Protection](#) im AWS CloudFormation Benutzerhandbuch.

Verwaltung der verwendeten Web-ACLs mit automatischer Schadensbegrenzung

Shield Advanced verwaltet die automatische Abwehr für Ihre geschützte Ressource mithilfe einer Regelgruppenregel in der AWS WAF Web-ACL der geschützten Ressource. Über die AWS WAF Konsole und die APIs wird die Regel in Ihren Web-ACL-Regeln aufgeführt, deren Name mit `ShieldMitigationRuleGroup` beginnt. Diese Regel ist Ihrer automatischen DDoS-Abwehr auf Anwendungsebene gewidmet und wird von Shield Advanced und für Sie verwaltet. AWS WAF Weitere Informationen finden Sie unter [Die Shield Advanced-Regelgruppe](#) und [So verwaltet Shield Advanced die automatische Schadensbegrenzung](#).

Wenn Sie Ihre Web-ACLs AWS CloudFormation zur Verwaltung Ihrer Web-ACLs verwenden, fügen Sie die Shield Advanced-Regelgruppenregel nicht zu Ihrer Web-ACL-Vorlage hinzu. Wenn Sie eine Web-ACL aktualisieren, die mit Ihren automatischen Schutzmaßnahmen verwendet wird, verwaltet AWS WAF automatisch die Regelgruppenregel in der Web-ACL.

Im Vergleich zu anderen Web-ACLs, die Sie verwalten, werden Sie die folgenden Unterschiede feststellen: AWS CloudFormation

- AWS CloudFormation meldet keine Abweichung im Stack-Drift-Status zwischen der tatsächlichen Konfiguration der Web-ACL mit der Shield Advanced-Regelgruppenregel und Ihrer Web-ACL-Vorlage ohne die Regel. Die Shield Advanced-Regel wird nicht in der tatsächlichen Liste für die Ressource in den Drift-Details angezeigt.

Sie können die Shield Advanced-Regelgruppenregel in Web-ACL-Auflistungen sehen AWS WAF, aus denen Sie sie abrufen, z. B. über die AWS WAF Konsole oder AWS WAF APIs.

- Wenn Sie die Web-ACL-Vorlage in einem Stapel ändern AWS WAF und Shield Advanced automatisch die automatische Abwehrregel von Shield Advanced in der aktualisierten Web-ACL beibehalten. Die von Shield Advanced bereitgestellten automatischen Schutzmaßnahmen zur Schadensbegrenzung werden durch Ihr Update der Web-ACL nicht unterbrochen.

Verwalten Sie die Shield Advanced-Regel nicht in Ihrer AWS CloudFormation Web-ACL-Vorlage. Die Web-ACL-Vorlage sollte die Shield Advanced-Regel nicht auflisten. Folgen Sie den bewährten Methoden für das Web-ACL-Management unter [Bewährte Methoden für die Verwendung der automatischen Schadensbegrenzung](#).

Gesundheitsbasierte Erkennung mithilfe von Gesundheitschecks

Sie können Shield Advanced so konfigurieren, dass es eine gesundheitsbasierte Erkennung verwendet, um die Reaktionsfähigkeit und Genauigkeit bei der Erkennung und Abwehr von Angriffen zu verbessern. Sie können diese Option für jeden Ressourcentyp außer für gehostete Route 53-Zonen verwenden.

Um die zustandsbasierte Erkennung zu konfigurieren, definieren Sie eine Zustandsprüfung für Ihre Ressource in Route 53, stellen sicher, dass sie als fehlerfrei gemeldet wird, und verknüpfen sie dann mit Ihrem Shield Advanced-Schutz. Informationen zu Route 53-Zustandsprüfungen finden Sie unter [So überprüft Amazon Route 53 den Zustand Ihrer Ressourcen](#) und [Erstellen, Aktualisieren und Löschen von Zustandsprüfungen](#) im Amazon Route 53-Entwicklerhandbuch.

Note

Für den proaktiven Engagement-Support des Shield Response Teams (SRT) sind Gesundheitschecks erforderlich. Informationen zu proaktivem Engagement finden Sie unter [Konfiguration von proaktivem Engagement](#).

Gesundheitschecks messen den Zustand Ihrer Ressourcen auf der Grundlage der von Ihnen definierten Anforderungen. Der Status der Integritätsprüfung liefert wichtige Informationen zu den Erkennungsmechanismen von Shield Advanced, sodass sie besser auf den aktuellen Status Ihrer spezifischen Anwendungen reagieren können.

Sie können die zustandsbasierte Erkennung für jeden Ressourcentyp aktivieren, mit Ausnahme von Route 53-Hosting-Zonen.

- Ressourcen auf Netzwerk- und Transportebene (Layer 3/Layer 4) — Health-based Detection verbessert die Genauigkeit der Erkennung und Abwehr von Ereignissen auf Netzwerk- und Transportebene für Network Load Balancer, Elastic IP-Adressen und Global Accelerator-Standardbeschleuniger. Wenn Sie diese Ressourcentypen mit Shield Advanced schützen, kann Shield Advanced Abwehr für kleinere Angriffe und schnellere Abwehr von Angriffen bieten, selbst wenn der Datenverkehr innerhalb der Kapazität der Anwendung liegt.

Wenn Sie eine zustandsbasierte Erkennung hinzufügen, kann Shield Advanced in Zeiten, in denen die zugehörige Zustandsprüfung fehlerhaft ist, Schutzmaßnahmen noch schneller und bei noch niedrigeren Schwellenwerten vornehmen.

- Ressourcen auf Anwendungsebene (Schicht 7) — Die auf Integrität basierende Erkennung verbessert die Genauigkeit der Erkennung von Fluten von Webanfragen für CloudFront Distributionen und Application Load Balancer. Wenn Sie diese Ressourcentypen mit Shield Advanced schützen, erhalten Sie Warnmeldungen zur Flutererkennung von Webanfragen, wenn es eine statistisch signifikante Abweichung im Verkehrsvolumen gibt, die mit signifikanten Änderungen der Verkehrsmuster kombiniert wird, basierend auf den Anforderungsmerkmalen.

Wenn die zugehörige Route 53-Zustandsprüfung fehlerhaft ist, benötigt Shield Advanced dank zustandsbasierter Erkennung kleinere Abweichungen, um eine Warnung zu erhalten, und Ereignisse werden schneller gemeldet. Umgekehrt, wenn die zugehörige Route 53-Zustandsprüfung fehlerfrei ist, benötigt Shield Advanced größere Abweichungen, um eine Warnung auszulösen.

Inhalt

- [Bewährte Methoden für die Verwendung von Gesundheitschecks mit Shield Advanced](#)
- [Metriken, die häufig für Gesundheitschecks verwendet werden](#)
 - [Metriken, die zur Überwachung des Anwendungszustands verwendet werden](#)
 - [CloudWatch Amazon-Metriken für jeden Ressourcentyp](#)
- [Verwaltung von Gesundheitscheckverbänden](#)
 - [Ihrer Ressource einen Integritätscheck zuordnen](#)
 - [Trennen Sie die Zuordnung eines Gesundheitschecks zu Ihrer Ressource](#)
 - [Der Status der Zugehörigkeit zur Gesundheitsprüfung](#)

- [Beispiele Health Gesundheitschecks](#)
 - [CloudFront Amazon-Verteilungen](#)
 - [Load Balancers](#)
 - [Elastische Amazon EC2 EC2-IP-Adresse \(EIP\)](#)

Bewährte Methoden für die Verwendung von Gesundheitschecks mit Shield Advanced

Folgen Sie den bewährten Methoden in diesem Abschnitt, wenn Sie Gesundheitschecks mit Shield Advanced erstellen und verwenden.

- Planen Sie Ihre Integritätsprüfungen, indem Sie die Komponenten Ihrer Infrastruktur identifizieren, die Sie überwachen möchten. Ziehen Sie die folgenden Ressourcentypen für Integritätsprüfungen in Betracht:
 - Kritische Ressourcen.
 - Alle Ressourcen, bei denen Sie eine höhere Sensitivität für die Erkennung und Abwehr von Shield Advanced wünschen.
 - Ressourcen, für die Shield Advanced Sie proaktiv kontaktieren soll. Das proaktive Engagement hängt vom Status Ihrer Gesundheitschecks ab.

Zu den Ressourcen, die Sie möglicherweise überwachen möchten, gehören CloudFront Amazon-Distributionen, mit dem Internet verbundene Load Balancer und Amazon EC2-Instances.

- Definieren Sie Integritätsprüfungen, die den Zustand Ihrer Anwendung genau wiedergeben und so wenige Benachrichtigungen wie möglich enthalten.
 - Schreiben Sie Integritätsprüfungen so, dass sie nur dann fehlerhaft sind, wenn Ihre Anwendung nicht verfügbar ist oder nicht innerhalb akzeptabler Parameter funktioniert. Sie sind dafür verantwortlich, Zustandsprüfungen auf der Grundlage der spezifischen Anforderungen Ihrer Anwendung zu definieren und durchzuführen.
 - Verwenden Sie so wenige Zustandsprüfungen wie möglich und berichten Sie dennoch genau über den Zustand Ihrer Anwendung. Beispielsweise können mehrere Alarme aus mehreren Bereichen Ihrer Anwendung, die alle dasselbe Problem melden, Ihre Reaktionsaktivitäten unnötig belasten, ohne dass ein zusätzlicher Informationswert entsteht.
 - Verwenden Sie berechnete Zustandsprüfungen, um den Zustand von Anwendungen anhand einer Kombination von CloudWatch Amazon-Metriken zu überwachen. Sie können beispielsweise die kombinierte Systemintegrität auf der Grundlage der Latenz Ihrer

Anwendungsserver und ihrer Fehlerraten von 5xx berechnen, was darauf hindeutet, dass der Ursprungsserver die Anfrage nicht erfüllt hat.

- Erstellen und veröffentlichen Sie nach Bedarf Ihre eigenen Anwendungszustandsindikatoren in Form von CloudWatch benutzerdefinierten Messwerten und verwenden Sie diese in einer berechneten Zustandsprüfung.
- Implementieren und verwalten Sie Ihre Integritätsprüfungen, um die Erkennung zu verbessern und unnötige Wartungsarbeiten zu reduzieren.
- Bevor Sie einen Gesundheitscheck mit einem Shield Advanced-Schutz verknüpfen, stellen Sie sicher, dass er sich in einem fehlerfreien Zustand befindet. Wenn Sie eine Zustandsprüfung zuordnen, die als fehlerhaft gemeldet wird, kann dies die Erkennungsmechanismen von Shield Advanced für Ihre geschützten Ressourcen verzerren.
- Halten Sie Ihre Gesundheitschecks für Shield Advanced verfügbar. Löschen Sie keine Zustandsprüfung in Route 53, die Sie für einen Shield Advanced-Schutz verwenden.
- Verwenden Sie Staging- und Testumgebungen nur, um Ihre Integritätsprüfungen zu testen. Pflegen Sie Integritätsprüfungszuordnungen nur für Umgebungen, die Leistung und Verfügbarkeit auf Produktionsebene erfordern. Behalten Sie in Shield Advanced für Staging- und Testumgebungen keine Integritätsprüfzuordnungen bei.

Metriken, die häufig für Gesundheitschecks verwendet werden

In diesem Abschnitt sind die CloudWatch Amazon-Metriken aufgeführt, die häufig bei Integritätsprüfungen verwendet werden, um den Zustand von Anwendungen bei Distributed-Denial-of-Service-Ereignissen (DDoS) zu messen. Vollständige Informationen zu den CloudWatch Metriken für jeden Ressourcentyp finden Sie in der Liste, die der Tabelle folgt.

Themen

- [Metriken, die zur Überwachung des Anwendungszustands verwendet werden](#)
- [CloudWatch Amazon-Metriken für jeden Ressourcentyp](#)

Metriken, die zur Überwachung des Anwendungszustands verwendet werden

Ressource	Metrik	Beschreibung
Route 53	HealthCheckStatus	Der Status des Endpunkts für die Integritätsprüfung.

Ressource	Metrik	Beschreibung
CloudFront	5xxErrorRate	Der Prozentsatz aller Anfragen, für die der HTTP-Statuscode 5xx lautet. Dies deutet auf einen Angriff hin, der sich auf die Anwendung auswirkt.
Application Load Balancer	ActiveConnectionCount	Die Anzahl der gleichzeitigen TCP-Verbindungen, die von Clients zum Load Balancer und vom Load Balancer zu Zielen aktiv sind.
Application Load Balancer	ConsumedLCUs	Anzahl von Load Balancer-Kapazitätseinheiten (LCU), die von Ihrem Load Balancer verwendet werden.
Application Load Balancer	HTTPCode_ELB_4XX_Count HTTPCode_ELB_5XX_Count	Die Anzahl der vom Load Balancer generierten HTTP-Fehlercodes des Typs 4xx oder 5xx.
Application Load Balancer	NewConnectionCount	Die Anzahl der neuen TCP-Verbindungen, die von Clients zum Load Balancer und vom Load Balancer zu Zielen hergestellt wurden.
Application Load Balancer	ProcessedBytes	Die Anzahl der vom Load Balancer verarbeiteten Byte.

Ressource	Metrik	Beschreibung
Application Load Balancer	RejectedConnectionCount	Die Anzahl der Verbindungen, die zurückgewiesen wurden, weil der Load Balancer seine maximale Anzahl von Verbindungen erreicht hat.
Application Load Balancer	TargetConnectionErrorCount	Die Anzahl der Verbindungen, die zwischen dem Load Balancer und dem Ziel nicht erfolgreich hergestellt wurden.
Application Load Balancer	TargetResponseTime	Die verstrichene Zeit in Sekunden, nachdem die Anfrage den Load Balancer verlassen hat und eine Antwort vom Ziel erhalten hat.
Application Load Balancer	UnHealthyHostCount	Die Anzahl der als instabil betrachteten Ziele.
Network Load Balancer	ActiveFlowCount	Die Anzahl gleichzeitiger TCP-Verbindungen von Clients zu Zielen.
Network Load Balancer	ConsumedLCUs	Anzahl von Load Balancer-Kapazitätseinheiten (LCU), die von Ihrem Load Balancer verwendet werden.
Network Load Balancer	NewFlowCount	Die Anzahl der neuen TCP-Verbindungen, die von Clients zu Zielen hergestellt wurden.

Ressource	Metrik	Beschreibung
Network Load Balancer	PeakPacketsPerSecond	Die höchste durchschnittliche Paketrate (pro Sekunde verarbeitete Pakete), berechnet alle 10 Sekunden während des Stichprobenfensters. Diese Metrik enthält den Datenverkehr mit Zustandsprüfungen.
Network Load Balancer	ProcessedBytes	Die Anzahl der vom Load Balancer verarbeiteten Byte, einschließlich TCP/IP-Headern.
Global Accelerator	NewFlowCount	Die Anzahl der neuen TCP-Verbindungen, die von Clients zu Zielen hergestellt wurden.
Global Accelerator	ProcessedBytesIn	Die Anzahl der vom Beschleuniger verarbeiteten eingehenden Byte, einschließlich TCP/IP-Headern.
Amazon EC2	CPUUtilization	Der Prozentsatz der zugewiesenen EC2-Rechenheiten, die derzeit verwendet werden.
Amazon EC2	NetworkIn	Anzahl der von der Instance auf allen Netzwerkschnittstellen empfangenen Byte.
Amazon EC2 Auto Scaling	GroupMaxSize	Die maximale Größe der Auto-Scaling-Gruppe.

CloudWatch Amazon-Metriken für jeden Ressourcentyp

Weitere Informationen zu den Metriken, die für Ihre geschützten Ressourcen verfügbar sind, finden Sie in den folgenden Abschnitten der Ressourcenhandbücher:

- Amazon Route 53 — [Überwachung Ihrer Ressourcen mit Amazon Route 53-Zustandsprüfungen und Amazon CloudWatch](#) im Amazon Route 53-Entwicklerhandbuch.
- Amazon CloudFront — [Monitoring CloudFront mit Amazon CloudWatch](#) im Amazon CloudFront Developer Guide.
- Application Load Balancer — [CloudWatch Metriken für Ihren Application Load Balancer](#) im Benutzerhandbuch für Application Load Balancer.
- Network Load Balancer — [CloudWatch Metriken für Ihren Network Load Balancer](#) im Benutzerhandbuch für Network Load Balancer.
- AWS Global Accelerator — [Verwendung von Amazon CloudWatch mit AWS Global Accelerator](#) im AWS Global Accelerator Developer Guide.
- Amazon Elastic Compute Cloud — [Listet die verfügbaren CloudWatch Metriken für Ihre Instances](#) im <https://docs.aws.amazon.com/AWSEC/UserGuide/2/latest/auf>.
- Amazon EC2 Auto Scaling — [CloudWatch Monitoring-Metriken für Ihre Auto Scaling Scoping-Gruppen und -Instances](#) im Amazon EC2 Auto Scaling Scoping-Benutzerhandbuch.

Verwaltung von Gesundheitscheckverbänden

Sie profitieren am meisten von der Verwendung einer Integritätsprüfung mit Shield Advanced, wenn die Integritätsprüfung nur dann fehlerfrei meldet, wenn Ihre Anwendung innerhalb akzeptabler Parameter läuft, und nur dann fehlerhaft meldet, wenn dies nicht der Fall ist. Verwenden Sie die Anleitungen in diesem Abschnitt, um Ihre Zuordnungen für Gesundheitsprüfungen in Shield Advanced zu verwalten.

Note

Shield Advanced verwaltet Ihre Gesundheitschecks nicht automatisch.

Folgendes ist erforderlich, um einen Gesundheitscheck mit Shield Advanced zu verwenden:

- Der Gesundheitscheck muss als fehlerfrei gemeldet werden, wenn Sie ihn mit Ihrem Shield Advanced-Schutz verknüpfen.

- Der Gesundheitscheck muss für den Zustand Ihrer geschützten Ressource relevant sein. Sie sind dafür verantwortlich, Integritätsprüfungen zu definieren und durchzuführen, mit denen der Zustand Ihrer Anwendung auf der Grundlage der spezifischen Anforderungen Ihrer Anwendung genau gemeldet wird.
- Der Gesundheitscheck muss weiterhin für den Shield Advanced-Schutz verfügbar sein. Löschen Sie keine Zustandsprüfung in Route 53, die Sie für einen Shield Advanced-Schutz verwenden.

Themen

- [Ihrer Ressource einen Integritätscheck zuordnen](#)
- [Trennen Sie die Zuordnung eines Gesundheitschecks zu Ihrer Ressource](#)
- [Der Status der Zugehörigkeit zur Gesundheitsprüfung](#)

Ihrer Ressource einen Integritätscheck zuordnen

Das folgende Verfahren zeigt, wie Sie eine Amazon Route 53-Zustandsprüfung mit einer geschützten Ressource verknüpfen.


Note

Bevor Sie einen Gesundheitscheck mit einem Shield Advanced-Schutz verknüpfen, stellen Sie sicher, dass er sich in einem fehlerfreien Zustand befindet. Weitere Informationen finden Sie im Amazon Route 53 Developer Guide unter [Überwachen des Status von Zustandsprüfungen und Empfangen von Benachrichtigungen](#).

So ordnen Sie einen Gesundheitscheck zu

1. Melden Sie sich bei der AWS WAF & Shield-Konsole an AWS Management Console und öffnen Sie sie unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im AWS Shield Navigationsbereich die Option Geschützte Ressourcen aus.
3. Wählen Sie auf der Registerkarte Schutz die Ressource aus, die Sie einer Integritätsprüfung zuordnen möchten.
4. Wählen Sie Schutzmaßnahmen konfigurieren aus.
5. Wählen Sie Weiter, bis Sie zur Seite DDoS-Erkennung auf Basis von Integritätsprüfungen konfigurieren — optional gelangen.

6. Wählen Sie unter Associated Health Check (Zugehörige Zustandsprüfung) die ID der Zustandsprüfung aus, die Sie der Schutzvorkehrung zuordnen möchten.

 Note

Wenn Sie die benötigte Zustandsprüfung nicht sehen, rufen Sie die Route 53-Konsole auf und überprüfen Sie die Zustandsprüfung und ihre ID. Weitere Informationen finden Sie unter [Erstellen und Aktualisieren von Zustandsprüfungen](#).

7. Gehen Sie die restlichen Seiten durch, bis Sie die Konfiguration abgeschlossen haben. Auf der Seite Schutzmaßnahmen ist Ihr aktualisierter Health Check-Link für die Ressource aufgeführt.
8. Prüfen Sie auf der Seite Schutzmaßnahmen, ob Ihr neu zugeordneter Gesundheitscheck als fehlerfrei gemeldet wird.

Sie können einen Gesundheitscheck in Shield Advanced nicht erfolgreich verwenden, solange der Gesundheitscheck als fehlerhaft gemeldet wird. Dies führt dazu, dass Shield Advanced bei sehr niedrigen Schwellenwerten falsch positive Ergebnisse erkennt, was sich auch negativ auf die Fähigkeit des Shield Response Teams (SRT) auswirken kann, die Ressource proaktiv einzusetzen.

Wenn die neu zugeordnete Zustandsprüfung als fehlerhaft gemeldet wird, gehen Sie wie folgt vor:

- a. Trennen Sie den Gesundheitscheck von Ihrem Schutz in Shield Advanced.
- b. Überprüfen Sie Ihre Health Check-Spezifikationen in Amazon Route 53 erneut und überprüfen Sie die allgemeine Leistung und Verfügbarkeit Ihrer Anwendung.
- c. Wenn Ihre Anwendung innerhalb Ihrer Gesundheitsparameter arbeitet und Ihr Gesundheitscheck als fehlerfrei gemeldet wird, versuchen Sie erneut, die Zustandsprüfung in Shield Advanced zu verknüpfen.

Das Verfahren der Health Check Association ist abgeschlossen, wenn Sie Ihre neue Health Check Association eingerichtet haben und sie in Shield Advanced als gesund gemeldet wird.

Trennen Sie die Zuordnung eines Gesundheitschecks zu Ihrer Ressource

Das folgende Verfahren zeigt, wie Sie eine Amazon Route 53-Zustandsprüfung von einer geschützten Ressource trennen.

So trennen Sie die Zuordnung einer Integritätsprüfung

1. Melden Sie sich bei der AWS WAF & Shield-Konsole an AWS Management Console und öffnen Sie sie unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im AWS Shield Navigationsbereich die Option Geschützte Ressourcen aus.
3. Wählen Sie auf der Registerkarte Schutz die Ressource aus, die Sie von einer Integritätsprüfung trennen möchten.
4. Wählen Sie Schutzmaßnahmen konfigurieren aus.
5. Wählen Sie Weiter, bis Sie zur Seite DDoS-Erkennung auf Basis von Integritätsprüfungen konfigurieren — optional gelangen.
6. Wählen Sie unter Associated Health Check die leere Option aus, die als - aufgeführt ist.
7. Gehen Sie die restlichen Seiten durch, bis Sie die Konfiguration abgeschlossen haben.

Auf der Seite Schutzmaßnahmen ist das Feld für die Integritätsprüfung für Ihre Ressource auf - gesetzt, was bedeutet, dass es keine Zuordnung zur Integritätsprüfung gibt.

Der Status der Zugehörigkeit zur Gesundheitsprüfung

Sie können den Status der Zustandsprüfung, die einem Schutz zugeordnet ist, auf der Seite Geschützte Ressourcen der AWS WAF & Shield-Konsole und auf der Detailseite jeder Ressource einsehen.

- Fehlerfrei — Der Gesundheitscheck ist verfügbar und wird als fehlerfrei gemeldet.
- Ungesund — Der Gesundheitscheck ist verfügbar und wird als ungesund gemeldet.
- Nicht verfügbar — Der Gesundheitscheck ist für Shield Advanced nicht verfügbar.

Um eine Zustandsprüfung „Nicht verfügbar“ zu beheben

Erstellen und verwenden Sie einen neuen Gesundheitscheck. Versuchen Sie nicht erneut, einen Gesundheitscheck zuzuordnen, nachdem er in Shield Advanced den Status Nicht verfügbar hatte.

Eine ausführliche Anleitung zur Durchführung dieser Schritte finden Sie in den vorangegangenen Themen.

1. Trennen Sie in Shield Advanced die Zustandsprüfung von der Ressource.

2. Erstellen Sie in Route 53 eine neue Zustandsprüfung für die Ressource und notieren Sie sich deren ID. Weitere Informationen finden Sie unter [Erstellen und Aktualisieren von Zustandsprüfungen](#) im Amazon Route 53-Entwicklerhandbuch.
3. Ordnen Sie in Shield Advanced den neuen Gesundheitscheck der Ressource zu.

Beispiele Health Gesundheitschecks

In diesem Abschnitt finden Sie Beispiele für Zustandsprüfungen, die Sie bei einer berechneten Zustandsprüfung verwenden könnten. Bei einer berechneten Zustandsprüfung wird anhand einer Reihe einzelner Zustandsprüfungen ein kombinierter Status ermittelt. Der Status jeder einzelnen Zustandsprüfung basiert auf dem Zustand eines Endpunkts oder auf dem Status einer CloudWatch Amazon-Metrik. Sie kombinieren Gesundheitschecks zu einem berechneten Zustandscheck und konfigurieren dann Ihren berechneten Zustandscheck so, dass der Gesundheitszustand auf der Grundlage des kombinierten Gesundheitsstatus der einzelnen Gesundheitschecks gemeldet wird. Passen Sie die Sensitivität Ihrer berechneten Zustandsprüfungen an Ihre Anforderungen an Anwendungsleistung und Verfügbarkeit an.

Informationen zu berechneten Zustandsprüfungen finden Sie unter [Überwachung anderer Zustandsprüfungen \(berechnete Zustandsprüfungen\)](#) im Amazon Route 53-Entwicklerhandbuch. Weitere Informationen finden Sie im Blogbeitrag [Route 53 Improvements — Calculated Health Checks and Latency Checks](#).

Themen

- [CloudFront Amazon-Verteilungen](#)
- [Load Balancers](#)
- [Elastische Amazon EC2 EC2-IP-Adresse \(EIP\)](#)

CloudFront Amazon-Verteilungen

In den folgenden Beispielen werden Zustandsprüfungen beschrieben, die zu einer berechneten Zustandsprüfung für eine CloudFront Verteilung kombiniert werden könnten:

- Überwachen Sie einen Endpunkt, indem Sie einen Domainnamen für einen Pfad auf der Distribution angeben, der dynamische Inhalte bereitstellt. Eine fehlerfreie Antwort würde die HTTP-Antwortcodes 2xx und 3xx beinhalten.
- Überwachen Sie den Status eines CloudWatch Alarms, der den Zustand des Ursprungs misst. CloudFront Sie können beispielsweise einen CloudWatch Alarm für die Application Load Balancer

Balancer-Metrik `TargetResponseTime` verwalten und eine Integritätsprüfung erstellen, die den Status des Alarms widerspiegelt. Die Integritätsprüfung kann fehlerhaft sein, wenn die Antwortzeit zwischen der Anfrage, die den Load Balancer verlässt, und dem Empfang einer Antwort vom Ziel, den im Alarm konfigurierten Schwellenwert überschreitet.

- Überwachen Sie den Status eines CloudWatch Alarms, der den Prozentsatz der Anfragen misst, für die der HTTP-Statuscode der Antwort 5xx lautet. Wenn die CloudFront 5xx-Fehlerrate der Verteilung höher als der im CloudWatch Alarm definierte Schwellenwert ist, wechselt der Status dieser Zustandsprüfung auf fehlerhaft.

Load Balancers

In den folgenden Beispielen werden Integritätsprüfungen beschrieben, die in berechneten Integritätsprüfungen für einen Application Load Balancer, Network Load Balancer oder Global Accelerator Standard Accelerator verwendet werden könnten.

- Überwachen Sie den Status eines CloudWatch Alarms, der die Anzahl der neuen Verbindungen misst, die von Clients zum Load Balancer hergestellt wurden. Sie können den Alarmschwellenwert für die durchschnittliche Anzahl neuer Verbindungen so einstellen, dass er bis zu einem gewissen Grad über Ihrem Tagesdurchschnitt liegt. Die Messwerte für jeden Ressourcentyp lauten wie folgt:
 - Application Load Balancer: `NewConnectionCount`
 - Network Load Balancer: `ActiveFlowCount`
 - Globaler Beschleuniger: `NewFlowCount`
- Überwachen Sie für Application Load Balancer und Network Load Balancer den Status eines CloudWatch Alarms, der die Anzahl der Load Balancer misst, die als fehlerfrei gelten. Sie können den Alarmschwellenwert entweder für die Availability Zone oder für die Mindestanzahl fehlerfreier Hosts festlegen, die Ihr Load Balancer benötigt. Die verfügbaren Metriken für die Load Balancer-Ressourcen lauten wie folgt:
 - Application Load Balancer: `HealthyHostCount`
 - Network Load Balancer: `HealthyHostCount`
- Überwachen Sie für Application Load Balancer den Status eines CloudWatch Alarms, der die Anzahl der HTTP 5xx-Antwortcodes misst, die von den Load Balancer-Zielen generiert wurden. Für einen Application Load Balancer können Sie die Metrik verwenden `HTTPCode_Target_5XX_Count` und den Alarmschwellenwert auf der Summe aller 5xx-Fehler für den Load Balancer basieren.

Elastische Amazon EC2 EC2-IP-Adresse (EIP)

Die folgenden Beispiel-Zustandsprüfungen könnten zu einer berechneten Zustandsprüfung für eine Amazon EC2 EC2-Elastic-IP-Adresse kombiniert werden:

- Überwachen Sie einen Endpunkt, indem Sie eine IP-Adresse für die Elastic IP-Adresse angeben. Die Zustandsprüfung bleibt fehlerfrei, solange eine TCP-Verbindung mit der Ressource hinter der IP-Adresse hergestellt werden kann.
- Überwachen Sie den Status eines CloudWatch Alarms, der den Prozentsatz der zugewiesenen Amazon EC2 EC2-Recheneinheiten misst, die derzeit auf der Instance verwendet werden. Sie können die Amazon EC2-Metrik verwenden `CPUUtilization` und den Alarmschwellenwert auf einer Ihrer Meinung nach hohen CPU-Auslastung für Ihre Anwendung basieren, z. B. 90%.

Verwaltung des Ressourcenschutzes in AWS Shield Advanced

Verwenden Sie die Anleitungen in diesem Abschnitt, um die Shield Advanced-Schutzmaßnahmen für Ihre Ressourcen zu verwalten.

Note

Shield Advanced schützt nur Ressourcen, die Sie entweder in Shield Advanced oder durch eine AWS Firewall Manager Shield Advanced-Richtlinie angegeben haben. Ihre Ressourcen werden nicht automatisch geschützt.

Wenn Sie eine AWS Firewall Manager Shield Advanced-Richtlinie verwenden, müssen Sie den Schutz für Ressourcen, die in den Geltungsbereich der Richtlinie fallen, nicht verwalten. Firewall Manager verwaltet automatisch den Schutz für Konten und Ressourcen, die in den Geltungsbereich einer Richtlinie fallen, entsprechend der Richtlinienkonfiguration. Weitere Informationen finden Sie unter [AWS Shield Advanced Richtlinien](#).

Themen

- [AWS Shield Advanced Schutz für Ressourcen hinzufügen AWS](#)
- [Schutzmaßnahmen konfigurieren AWS Shield Advanced](#)
- [AWS Shield Advanced Der Schutz einer AWS Ressource wird entfernt](#)

AWS Shield Advanced Schutz für Ressourcen hinzufügen AWS

Folgen Sie den Anweisungen in diesem Abschnitt, um Shield Advanced-Schutz zu einer oder mehreren Ressourcen hinzuzufügen.

Um Schutz für eine AWS Ressource hinzuzufügen

1. Melden Sie sich bei der AWS WAF & Shield-Konsole an AWS Management Console und öffnen Sie sie unter <https://console.aws.amazon.com/wafv2/>.
2. AWS Shield Wählen Sie im Navigationsbereich unter Geschützte Ressourcen aus.
3. Wählen Sie Zu schützende Ressourcen hinzufügen aus.
4. Geben Sie auf der Seite Ressourcen auswählen, die mit Shield Advanced geschützt werden sollen, unter Region und Ressourcentypen angeben die Regions- und Ressourcentypspezifikationen für die Ressourcen an, die Sie schützen möchten. Sie können Ressourcen in mehreren Regionen schützen, indem Sie Alle Regionen auswählen, und Sie können die Auswahl auf globale Ressourcen einschränken, indem Sie Global auswählen. Sie können alle Ressourcentypen abwählen, die Sie nicht schützen möchten. Informationen zum Schutz Ihrer Ressourcentypen finden Sie unter [AWS Shield Advanced Schutzmaßnahmen nach Ressourcentyp](#)
5. Wählen Sie Ressourcen laden aus. Shield Advanced füllt den Abschnitt Ressourcen auswählen mit den AWS Ressourcen, die Ihren Kriterien entsprechen.
6. Im Bereich Ressourcen auswählen können Sie die Ressourcenliste filtern, indem Sie eine Zeichenfolge eingeben, nach der in den Ressourcenlisten gesucht werden soll.

Wählen Sie die Ressourcen aus, die Sie schützen möchten.
7. Wenn Sie den von Ihnen erstellten Shield Advanced-Schutzmaßnahmen Tags hinzufügen möchten, geben Sie diese im Abschnitt Tags an. Informationen zum Markieren von AWS Ressourcen finden Sie unter [Arbeiten mit dem Tag-Editor](#).
8. Wählen Sie Protect with Shield Advanced. Dadurch werden die Ressourcen um Shield Advanced-Schutzmaßnahmen erweitert.

Schutzmaßnahmen konfigurieren AWS Shield Advanced

Sie können die Einstellungen für Ihre AWS Shield Advanced Schutzmaßnahmen jederzeit ändern. Gehen Sie dazu die Optionen für Ihre ausgewählten Schutzmaßnahmen durch und ändern Sie die Einstellungen, die Sie ändern müssen.

Um geschützte Ressourcen zu verwalten

1. Melden Sie sich bei der AWS WAF & Shield-Konsole an AWS Management Console und öffnen Sie sie unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im AWS Shield Navigationsbereich die Option Geschützte Ressourcen aus.
3. Wählen Sie auf der Registerkarte Schutz die Ressourcen aus, die Sie schützen möchten.
4. Wählen Sie Schutzmaßnahmen konfigurieren und wählen Sie die gewünschte Option für die Ressourcenspezifikation aus.
5. Gehen Sie die einzelnen Ressourcenschutzoptionen durch und nehmen Sie bei Bedarf Änderungen vor.

Konfigurieren Sie den DDoS-Schutz auf Anwendungsebene

Zum Schutz vor Angriffen auf Amazon CloudFront - und Application Load Balancer Balancer-Ressourcen können Sie AWS WAF Web-ACLs und ratenbasierte Regeln hinzufügen. Weitere Informationen hierzu finden Sie unter [Shield Advanced AWS WAF Web-ACLs und ratenbasierte Regeln auf Anwendungsebene](#).

Sie können auch die automatische DDoS-Abwehr auf Anwendungsebene von Shield Advanced aktivieren. Informationen darüber, wie das AWS WAF funktioniert, finden Sie unter [AWS WAF](#). Informationen zur automatischen Schadensbegrenzungsfunktion finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#).

Important

Wenn Sie Ihre Shield Advanced-Schutzmaßnahmen AWS Firewall Manager mithilfe einer Shield Advanced-Richtlinie verwalten, können Sie die Schutzmaßnahmen auf Anwendungsebene hier nicht verwalten. Für alle anderen Ressourcen empfehlen wir, dass Sie mindestens jeder Ressource eine Web-ACL zuordnen, auch wenn die Web-ACL keine Regeln enthält.

Note

Wenn Sie bei Bedarf die automatische DDoS-Abwehr auf Anwendungsebene für eine Ressource aktivieren, fügt der Vorgang Ihrem Konto automatisch eine serviceverknüpfte Rolle hinzu, um Shield Advanced die erforderlichen Berechtigungen zur Verwaltung Ihres


Web-ACL-Schutzes zu gewähren. Weitere Informationen finden Sie unter [Verwenden von serviceverknüpften Rollen für Shield Advanced](#).

Um den DDoS-Schutz auf Anwendungsebene zu konfigurieren

1. Wenn die Ressource noch nicht mit einer Web-ACL verknüpft ist, können Sie auf der Seite „DDoS-Schutz auf Ebene 7 konfigurieren“ eine bestehende Web-ACL auswählen oder eine eigene erstellen.

Führen Sie zur Erstellung einer Web-ACL die folgenden Schritte aus:

- a. Wählen Sie Create web ACL (Web-ACL erstellen) aus.
- b. Geben Sie einen Namen ein. Sie können den Namen nach dem Erstellen der Web-ACL nicht mehr ändern.
- c. Wählen Sie Erstellen.

 Note

Wenn eine Ressource bereits einer Web-ACL zugeordnet ist, können Sie nicht zu einer anderen Web-ACL wechseln. Wenn Sie die Web-ACL wechseln möchten, müssen Sie zunächst die zugeordneten Web-ACLs aus der Ressource entfernen. Weitere Informationen finden Sie unter [Zuordnen oder Aufheben der Zuordnung einer Web-ACL zu einer Ressource AWS](#).

2. Wenn für die Web-ACL keine ratenbasierte Regel definiert ist, können Sie eine hinzufügen, indem Sie Ratenbegrenzungsregel hinzufügen wählen und dann die folgenden Schritte ausführen:
 - a. Geben Sie einen Namen ein.
 - b. Geben Sie ein Durchsatzlimit ein. Dies ist die maximale Anzahl von Anfragen, die in einem Zeitraum von fünf Minuten von einer einzelnen IP-Adresse aus zulässig sind, bevor die ratenbasierte Regelaktion auf die IP-Adresse angewendet wird. Wenn die Anfragen von der IP-Adresse unter den Grenzwert fallen, wird die Aktion abgebrochen.
 - c. Stellen Sie die Regelaktion so ein, dass Anfragen von IP-Adressen gezählt oder blockiert werden, solange deren Anzahl der Anfragen das Limit überschreitet. Die Anwendung

und Entfernung der Regelaktion kann ein oder zwei Minuten nach der Änderung der IP-Adressanforderungsrate wirksam werden.

- d. Wählen Sie Regel hinzufügen aus.
3. Wählen Sie für Automatische DDoS-Abwehr auf Anwendungsebene wie folgt aus, ob Shield Advanced DDoS-Angriffe in Ihrem Namen automatisch abwehren soll:
 - Um die automatische Abwehr zu aktivieren, wählen Sie Aktivieren und dann die AWS WAF Regelaktion aus, die Shield Advanced in seinen benutzerdefinierten Regeln verwenden soll. Sie haben die Wahl zwischen Count und Block. Informationen zu diesen AWS WAF Regelaktionen finden Sie unter [Regelaktion](#). Informationen darüber, wie Shield Advanced diese Aktionseinstellung verwaltet, finden Sie unter [So verwaltet Shield Advanced die Einstellung für Regelaktionen](#).
 - Um die automatische Schadensbegrenzung zu deaktivieren, wählen Sie Deaktivieren.
 - Um die Einstellungen für die automatische Risikominderung für die Ressourcen, die Sie verwalten, unverändert zu lassen, behalten Sie die Standardauswahl Aktuelle Einstellungen beibehalten bei.

Informationen zur automatischen DDoS-Abwehr auf Anwendungsebene mit Shield Advanced finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#)

4. Wählen Sie Weiter aus.

Alarmer und Benachrichtigungen erstellen

Das folgende Verfahren zeigt, wie CloudWatch Alarmer für geschützte Ressourcen verwaltet werden.

Note

CloudWatch verursacht zusätzliche Kosten. CloudWatch Die Preise finden Sie unter [CloudWatch Amazon-Preise](#).

Um Alarmer und Benachrichtigungen zu erstellen

1. Konfigurieren Sie auf der Schutzseite Alarmer und Benachrichtigungen erstellen — optional die SNS-Themen für die Alarmer und Benachrichtigungen, die Sie erhalten möchten. Wählen Sie für Ressourcen, für die keine Benachrichtigungen erforderlich sind, No topic (Kein Thema) aus. Sie können ein Amazon SNS SNS-Thema hinzufügen oder ein neues Thema erstellen.

2. Gehen Sie folgendermaßen vor, um ein Amazon SNS SNS-Thema zu erstellen:
 - a. Wählen Sie in der Dropdownliste die Option Ein SNS-Thema erstellen aus.
 - b. Geben Sie einen Themennamen ein.
 - c. Geben Sie optional eine E-Mail-Adresse ein, an die die Amazon SNS SNS-Nachrichten gesendet werden, und wählen Sie dann E-Mail hinzufügen. Sie können mehr als eine eingeben.
 - d. Wählen Sie Erstellen.
3. Wählen Sie Weiter aus.

AWS Shield Advanced Der Schutz einer AWS Ressource wird entfernt

Sie können AWS Shield Advanced den Schutz für jede Ihrer AWS Ressourcen jederzeit aufheben.

Important

Durch das Löschen einer AWS Ressource wird die Ressource nicht von entfernt AWS Shield Advanced. Sie müssen auch den Schutz für die Ressource von entfernen AWS Shield Advanced, wie in diesem Verfahren beschrieben.

Entfernen Sie AWS Shield Advanced den Schutz von einer AWS Ressource

1. Melden Sie sich bei der AWS WAF & Shield-Konsole an AWS Management Console und öffnen Sie sie unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im AWS Shield Navigationsbereich die Option Geschützte Ressourcen aus.
3. Wählen Sie auf der Registerkarte Schutz die Ressourcen aus, deren Schutz Sie entfernen möchten.
4. Wählen Sie Schutzmaßnahmen löschen aus.
 - Wenn Sie einen CloudWatch Amazon-Alarm für einen Schutz konfiguriert haben, haben Sie die Möglichkeit, den Alarm zusammen mit dem Schutz zu löschen. Wenn Sie den Alarm zu diesem Zeitpunkt nicht löschen möchten, können Sie ihn stattdessen später über die CloudWatch Konsole löschen.

Note

Wenn Sie bei Schutzmaßnahmen, für die eine Amazon Route 53-Zustandsprüfung konfiguriert ist, den Schutz später erneut hinzufügen, beinhaltet der Schutz immer noch die Zustandsprüfung.

Mit den vorherigen Schritten wird der AWS Shield Advanced Schutz für bestimmte AWS Ressourcen aufgehoben. Sie kündigen Ihr AWS Shield Advanced Abonnement nicht. Dieser Service wird Ihnen weiterhin in Rechnung gestellt. Für Informationen zu Ihrem AWS Shield Advanced Abonnement wenden Sie sich an das [AWS Support Center](#).

Einen CloudWatch Alarm aus Ihrem Shield Advanced-Schutz entfernen

Um einen CloudWatch Alarm aus Ihrem Shield Advanced-Schutz zu entfernen, gehen Sie wie folgt vor:

- Löschen Sie den Schutz wie in [AWS Shield Advanced Der Schutz einer AWS Ressource wird entfernt](#) beschrieben. Deaktivieren Sie das Kontrollkästchen neben Also delete related DDoSDetection alarm (Auch zugehörigen DDoSDetection-Alarm löschen).
- Löschen Sie den Alarm mithilfe der CloudWatch Konsole. Der Name des zu löschenden Alarms beginnt mit DDoS DetectedAlarmForProtection.

AWS Shield Advanced Schutzgruppen

Verwenden Sie Schutzgruppen, um logische Sammlungen Ihrer geschützten Ressourcen zu erstellen und deren Schutz als Gruppe zu verwalten. Informationen zur Verwaltung von Ressourcenschutzmaßnahmen finden Sie unter [Schutzmaßnahmen konfigurieren AWS Shield Advanced](#)

Note

Die automatische DDoS-Abwehr auf Anwendungsebene interagiert nicht mit Schutzgruppen. Sie können die automatische Abwehr für Ressourcen aktivieren, die sich in Schutzgruppen befinden, aber Shield Advanced wendet nicht automatisch Angriffsabwehrmaßnahmen an,

die auf den Ergebnissen der Schutzgruppe basieren. Shield Advanced wendet automatische Angriffsabwehrmaßnahmen für einzelne Ressourcen an.

AWS Shield Advanced Schutzgruppen bieten Ihnen eine Self-Service-Möglichkeit, den Umfang der Erkennung und Abwehr individuell anzupassen, indem mehrere geschützte Ressourcen als eine einzige Einheit behandelt werden. Die Gruppierung von Ressourcen kann eine Reihe von Vorteilen bieten.

- Verbessern Sie die Erkennungsgenauigkeit.
- Reduzieren Sie Benachrichtigungen über Ereignisse, die nicht bearbeitet werden können.
- Erhöhen Sie den Umfang der Maßnahmen zur Schadensbegrenzung, sodass auch geschützte Ressourcen einbezogen werden, die bei einem Ereignis ebenfalls beeinträchtigt werden könnten.
- Beschleunigen Sie die Zeit bis zur Abwehr von Angriffen mit mehreren ähnlichen Zielen.
- Erleichtern Sie den automatischen Schutz neu erstellter geschützter Ressourcen.

Schutzgruppen können dazu beitragen, Fehlalarme in Situationen wie Blau/Grün-Swaps zu reduzieren, bei denen Ressourcen abwechselnd fast ausgelastet sind oder voll ausgelastet sind. Ein anderes Beispiel ist, wenn Sie Ressourcen häufig erstellen und löschen und dabei ein Lastniveau beibehalten, das von allen Mitgliedern der Gruppe gemeinsam genutzt wird. In solchen Situationen kann die Überwachung einzelner Ressourcen zu Fehlalarmen führen, die Überwachung des Zustands der Ressourcengruppe dagegen nicht.

Sie können Schutzgruppen so konfigurieren, dass sie alle geschützten Ressourcen, alle Ressourcen bestimmter Ressourcentypen oder individuell angegebene Ressourcen umfassen. Neu geschützte Ressourcen, die Ihre Schutzgruppenkriterien erfüllen, werden automatisch in Ihre Schutzgruppe aufgenommen. Eine geschützte Ressource kann mehreren Schutzgruppen angehören.

AWS Shield Advanced Schutzgruppen verwalten

Verwenden Sie die Anleitungen in diesem Abschnitt, um Ihre Schutzgruppenkonfigurationen zu verwalten.

Eine Shield Advanced-Schutzgruppe erstellen

Um eine Schutzgruppe zu erstellen

1. Melden Sie sich bei der AWS WAF & Shield-Konsole an AWS Management Console und öffnen Sie sie unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im AWS Shield Navigationsbereich die Option Geschützte Ressourcen aus.
3. Wählen Sie die Registerkarte Schutzgruppen und dann Schutzgruppe erstellen aus.
4. Geben Sie auf der Seite Schutzgruppe erstellen einen Namen für Ihre Gruppe ein. Sie verwenden diesen Namen, um die Gruppe in Ihrer Liste der geschützten Ressourcen zu identifizieren. Sie können den Namen einer Schutzgruppe nicht ändern, nachdem Sie sie erstellt haben.
5. Wählen Sie unter Schutzgruppierungskriterien die Kriterien aus, anhand derer Shield Advanced die geschützten Ressourcen identifiziert, die in die Gruppe aufgenommen werden sollen. Treffen Sie Ihre zusätzlichen Auswahlen auf der Grundlage der von Ihnen ausgewählten Kriterien.
6. Wählen Sie unter Aggregation aus, wie Shield Advanced die Ressourcendaten für die Gruppe kombinieren soll, um Ereignisse zu erkennen, zu mindern und zu melden.
 - Summe — Verwendet den gesamten Datenverkehr in der Gruppe. In den meisten Fällen ist dies eine gute Wahl. Beispiele hierfür sind Elastic IP-Adressen für Amazon EC2 EC2-Instances, die manuell oder automatisch skaliert werden.
 - Mittelwert — Es wird der Durchschnitt des Datenverkehrs innerhalb der Gruppe verwendet. Dies ist eine gute Wahl für Ressourcen, die den Traffic einheitlich teilen. Beispiele hierfür sind Beschleuniger und Load Balancer.
 - Max. — Nutzt den höchsten Traffic von jeder Ressource. Dies ist nützlich für Ressourcen, die den Verkehr nicht gemeinsam nutzen, und für Ressourcen, die den Verkehr auf ungleichmäßige Weise teilen. Beispiele hierfür sind CloudFront Amazon-Distributionen und Herkunftsressourcen für CloudFront Distributionen.
7. Wählen Sie Speichern, um Ihre Schutzgruppe zu speichern und zur Seite Geschützte Ressourcen zurückzukehren.

Auf der Seite Shield-Ereignisse können Sie Ereignisse für Ihre Schutzgruppe anzeigen und zusätzliche Informationen zu den geschützten Ressourcen in der Gruppe aufrufen.

Aktualisierung einer Shield Advanced-Schutzgruppe

Um eine Schutzgruppe zu aktualisieren

1. Melden Sie sich bei der AWS WAF & Shield-Konsole an AWS Management Console und öffnen Sie sie unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im AWS Shield Navigationsbereich die Option Geschützte Ressourcen aus.
3. Aktivieren Sie auf der Registerkarte Schutzgruppen das Kontrollkästchen neben der Schutzgruppe, die Sie ändern möchten.
4. Wählen Sie auf der Seite der Schutzgruppe die Option Bearbeiten aus. Nehmen Sie Ihre Änderungen an den Einstellungen der Schutzgruppe vor.
5. Wählen Sie Speichern, um Ihre Änderungen zu speichern.

Löschen einer Shield Advanced-Schutzgruppe

Um eine Schutzgruppe zu löschen

1. Melden Sie sich bei der AWS WAF & Shield-Konsole an AWS Management Console und öffnen Sie sie unter <https://console.aws.amazon.com/wafv2/>.
2. Wählen Sie im AWS Shield Navigationsbereich die Option Geschützte Ressourcen aus.
3. Aktivieren Sie auf der Registerkarte Schutzgruppen das Kontrollkästchen neben der Schutzgruppe, die Sie entfernen möchten.
4. Wählen Sie auf der Seite der Schutzgruppe die Option Löschen aus und bestätigen Sie die Aktion.

Verfolgung von Änderungen am Ressourcenschutz in AWS Config


Sie können Änderungen am AWS Shield Advanced Schutz Ihrer Ressourcen mit aufzeichnen AWS Config. Anschließend können Sie diese Informationen verwenden, um ein Protokoll der Konfigurationsänderungen für Audit- und Fehlerbehebungszwecke zu pflegen.

Um Schutzänderungen aufzuzeichnen, aktivieren Sie AWS Config die Option für jede Ressource, die Sie verfolgen möchten. Weitere Informationen finden Sie unter [Erste Schritte mit AWS Config](#) im AWS Config -Developerhandbuch.

Sie müssen die Aktivierung AWS Config für jede Ressource aktivieren AWS-Region , die die verfolgten Ressourcen enthält. Sie können die Option AWS Config manuell aktivieren oder die

AWS CloudFormation Vorlage „Aktivieren AWS Config“ unter [AWS CloudFormation StackSets Beispielvorgaben](#) im AWS CloudFormation Benutzerhandbuch verwenden.

Wenn Sie die Option aktivieren AWS Config, werden Ihnen die Gebühren gemäß den Angaben auf der Seite mit den [AWS Config Preisen](#) berechnet.

 Note

Wenn Sie die AWS Config Aktivierung bereits für die erforderlichen Regionen und Ressourcen aktiviert haben, müssen Sie nichts weiter tun. AWS Config Protokolle über Schutzänderungen an Ihren Ressourcen beginnen automatisch mit Daten zu füllen.

Verwenden Sie nach der Aktivierung AWS Config die Region USA Ost (Nord-Virginia) in der AWS Config Konsole, um den Verlauf der Konfigurationsänderungen für AWS Shield Advanced globale Ressourcen einzusehen.

Zeigen Sie den Änderungsverlauf für AWS Shield Advanced regionale Ressourcen über die AWS Config Konsole in den Regionen USA Ost (Nord-Virginia), USA Ost (Ohio), USA West (Oregon), USA West (Nordkalifornien), Europa (Irland), Europa (Frankfurt), Asien-Pazifik (Tokio) und Asien-Pazifik (Sydney) an.

Einblick in DDoS-Ereignisse

AWS Shield bietet Einblick in die folgenden Kategorien von Veranstaltungen und Veranstaltungsaktivitäten:

- Global — Alle Kunden können auf eine aggregierte Übersicht der weltweiten Bedrohungsaktivitäten der letzten zwei Wochen zugreifen. Sie finden diese Informationen auf den Seiten „Erste Schritte“ und „Globales Bedrohungs-Dashboard“ der AWS Shield Konsole. Weitere Informationen finden Sie unter [AWS Shield globale Aktivitäten und Kontoaktivitäten](#).
- Konto — Alle Kunden können auf eine Zusammenfassung der Ereignisse für ihr Konto im Vorjahr zugreifen. Sie finden diese Informationen auf der Seite „Erste Schritte“ der AWS Shield Konsole. Weitere Informationen finden Sie unter [AWS Shield globale Aktivitäten und Kontoaktivitäten](#).

Wenn Sie Shield Advanced abonnieren und Ihre Ressourcen schützen, erhalten Sie Zugriff auf zusätzliche Informationen über die Ereignisse und DDoS-Angriffe auf die geschützten Ressourcen:

- Ereignisse auf geschützten Ressourcen — Shield Advanced bietet detaillierte Informationen zu jedem Ereignis auf der Seite Ereignisse der AWS Shield Konsole. Weitere Informationen finden Sie unter [AWS Shield Advanced Ereignisse](#).
- Ereigniskennzahlen für geschützte Ressourcen — Shield Advanced veröffentlicht Erkennungs-, Schadensbegrenzungs- und CloudWatch Amazon-Statistiken zu allen Ressourcen, die es schützt. Sie können diese Metriken verwenden, um CloudWatch Dashboards und Alarme zu konfigurieren. Weitere Informationen finden Sie unter [AWS Shield Advanced Metriken](#).
- Kontoübergreifende Sichtbarkeit von Ereignissen für geschützte Ressourcen — Wenn Sie Ihre Shield Advanced-Schutzmaßnahmen verwalten, können Sie die Sichtbarkeit von Schutzmaßnahmen für mehrere Konten aktivieren, indem Sie den Firewall Manager in Kombination mit verwenden. AWS Firewall Manager AWS Security Hub Weitere Informationen finden Sie unter [Kontoübergreifende Sichtbarkeit von Ereignissen](#).

Wenn Sie die automatische DDoS-Abwehr auf Anwendungsebene für den Schutz auf Anwendungsebene aktivieren,

Themen

- [AWS Shield globale Aktivitäten und Kontoaktivitäten](#)
- [AWS Shield Advanced Ereignisse](#)
- [Kontoübergreifende Sichtbarkeit von Ereignissen](#)

AWS Shield globale Aktivitäten und Kontoaktivitäten

Auf den AWS Shield Konsolenseiten „Erste Schritte“ und „Globales Bedrohungs-Dashboard“ finden Sie eine aggregierte Ansicht der globalen Bedrohungsaktivitäten und eine Zusammenfassung der Ereignisse pro Konto.

Der folgende Screenshot zeigt ein Beispiel für eine Seite mit den ersten Schritten.

Security, Identity, and Compliance

AWS Shield

Managed DDoS protection service.

AWS Shield provides continuous attack detection and automatic mitigations. AWS Shield offers two tiers of protection - Standard and Advanced.

Get started with Shield Advanced

Subscribe and add resources that you want to protect with Shield Advanced.

[Add resources to protect](#)

Pricing (US)

Monthly \$3000 / month

Additional data transfer fees apply

[View pricing](#)

More resources

[Documentation](#)

[API reference](#)

[FAQs](#)

[Support forums](#)

Global activity detected by AWS Shield

The following is a summary of events detected by AWS Shield across all applications running on AWS. With AWS Shield Advanced, you also receive a dashboard that's specific to your applications.



Last two weeks summary

Largest packet attack	188 Mpps
Largest bit rate	428 Gbps
Most common vector	Volumetric
Threat level	Normal
Total number of attacks	41,990

Account activity detected by AWS Shield

Events summary in past year

Values are for interval 2019-10-27T00:00 UTC to 2020-10-27T00:00 UTC. The statistics refer to all of your resources that are supported by AWS Shield, both protected and unprotected.

8

Total events

45.2 Gbps

Largest bit rate

15.5 Mpps

Largest packet rate

1.2 krps

Largest request rate

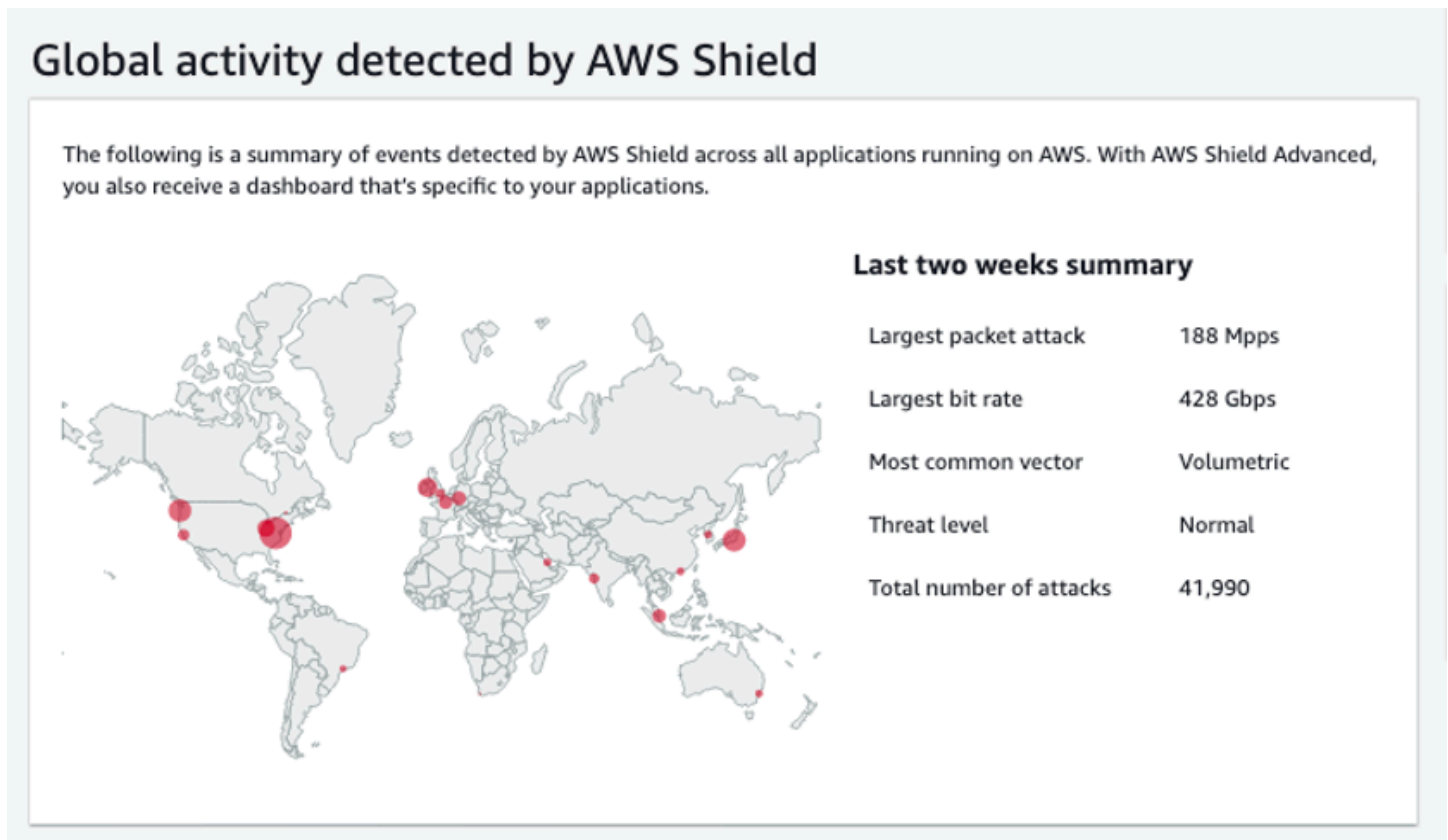
So greifen Sie auf die Konsole zu AWS Shield

- Melden Sie sich bei der AWS WAF & Shield-Konsole an AWS Management Console und öffnen Sie sie unter <https://console.aws.amazon.com/wafv2/>.

Sie benötigen kein Abonnement für Shield Advanced, um auf Informationen zu globalen Aktivitäten und Kontoereignissen zuzugreifen.

Weltweite Aktivitäten

Diese Informationen sind auf der AWS Shield Konsole über das globale Bedrohungs-Dashboard und auf den Seiten Erste Schritte verfügbar. Der folgende Screenshot zeigt ein Beispiel für den globalen Aktivitätsbereich.



Die globale Aktivität beschreibt DDoS-Ereignisse, die bei allen Kunden beobachtet wurden. AWS aktualisiert einmal pro Stunde die Informationen der letzten zwei Wochen. Im Konsolenbereich können Sie die Ergebnisse sehen, die nach AWS Regionen partitioniert und auf einer Welt-Heatmap angezeigt werden. Neben der Karte zeigt Shield zusammenfassende Informationen wie den größten Paketangriff, die größte Bitrate, den häufigsten Vektor, die Gesamtzahl der Angriffe und die Bedrohungsstufe an. Bei der Bedrohungsstufe handelt es sich um eine Bewertung der aktuellen weltweiten Aktivitäten im Vergleich zu dem, was AWS üblicherweise beobachtet wird. Der Standardwert für die Bedrohungsstufe ist Normal. AWS aktualisiert den Wert bei erhöhter DDoS-Aktivität automatisch auf Hoch.

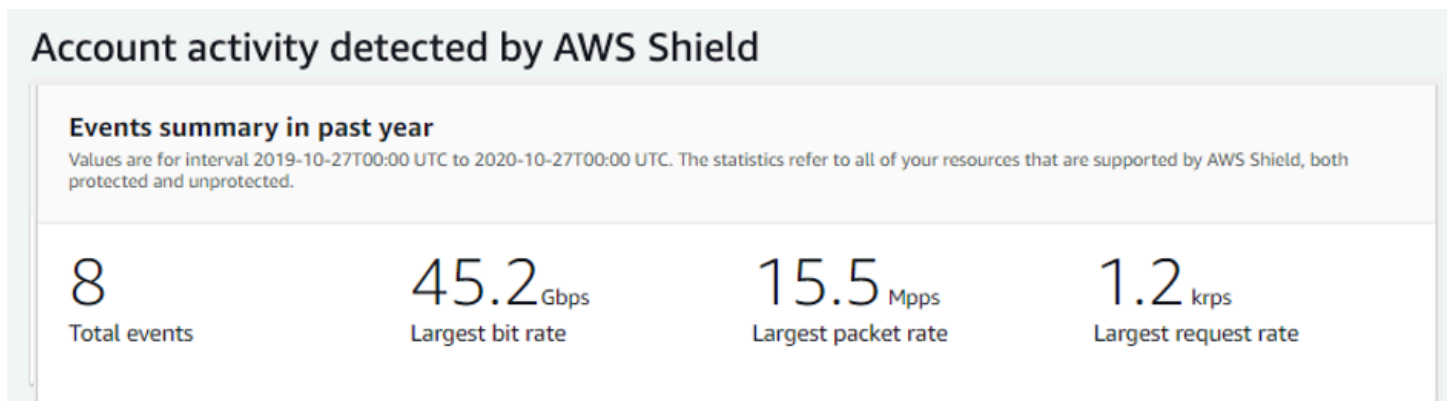
Das globale Bedrohungs-Dashboard bietet auch Zeitreihen-Metriken und gibt Ihnen die Möglichkeit, zwischen Zeitdauern zu wechseln. Um den Verlauf bedeutender DDoS-Angriffe einzusehen, können Sie das Dashboard so anpassen, dass es vom letzten Tag bis zu den letzten zwei Wochen angezeigt wird. Zeitreihen-Metriken bieten einen Überblick über die höchste Bitrate, Paketrate oder

Anforderungsrate für alle Ereignisse, die von AWS Shield Anwendungen erkannt wurden, auf denen AWS während des von Ihnen ausgewählten Zeitfensters ausgeführt wird.

Kontoaktivität

Diese Informationen sind auf der AWS Shield Konsoleseite „Erste Schritte“ verfügbar.

Der folgende Screenshot zeigt ein Beispiel für einen Bereich mit Kontoaktivitäten.



Kontoaktivität beschreibt DDoS-Ereignisse, die Shield für Ihre Ressourcen erkannt hat, die für den Schutz durch Shield Advanced in Frage kommen. Shield erstellt täglich zusammenfassende Kennzahlen für das Jahr, das am Vortag um 00:00 Uhr UTC endet, und zeigt dann die Gesamtzahl der Ereignisse, die größte Bitrate, die größte Paketrate und die größte Anforderungsrate an.

- Die Metrik zur Gesamtzahl der Ereignisse spiegelt jedes Mal wider, wenn Shield verdächtige Attribute im Datenverkehr entdeckte, der für Ihre Anwendung bestimmt war. Zu den verdächtigen Attributen können Datenverkehr gehören, der ein höheres Volumen als normal aufweist, Datenverkehr, der nicht dem historischen Profil Ihrer Anwendung entspricht, oder Verkehr, der nicht den von Shield für gültigen Anwendungsdatenverkehr definierten Heuristiken entspricht.
- Statistiken zur größten Bitrate und zur größten Paketrate sind für jede Ressource verfügbar.
- Die Statistik mit der höchsten Anforderungsrate ist nur für CloudFront Amazon-Distributionen und Application Load Balancer verfügbar, denen eine Web-ACL zugeordnet AWS WAF ist.

Note

Sie können auch über den API-Vorgang auf die Zusammenfassung der Ereignisse auf Kontoebene zugreifen. AWS Shield [DescribeAttackStatistics](#)

AWS Shield Advanced Ereignisse

Wenn Sie Shield Advanced abonnieren und Ihre Ressourcen schützen, erhalten Sie Zugriff auf zusätzliche Sichtbarkeitsfunktionen für die Ressourcen. Dazu gehören Benachrichtigungen nahezu in Echtzeit über Ereignisse, die von Shield Advanced erkannt werden, sowie zusätzliche Informationen über erkannte Ereignisse und Abhilfemaßnahmen.

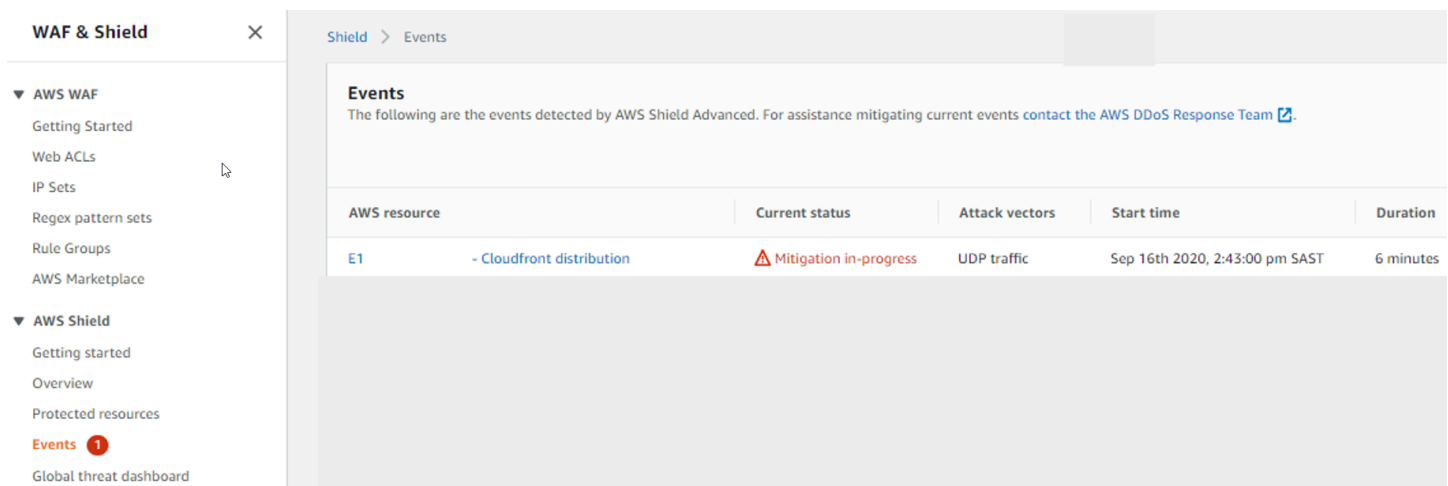
Note

Ihre Ereignisinformationen in der Shield Advanced-Konsole basieren auf Shield Advanced-Metriken. Informationen zu Shield Advanced-Metriken finden Sie unter [AWS Shield Advanced Metriken](#)

AWS Shield bewertet den Datenverkehr zu Ihrer geschützten Ressource anhand mehrerer Dimensionen. Wenn eine Anomalie erkannt wird, erstellt Shield Advanced für jede betroffene Ressource ein separates Ereignis.

Sie können über die Seite Ereignisse der Shield-Konsole auf Zusammenfassungen und Details zu den Ereignissen zugreifen. Die Seite „Ereignisse“ auf oberster Ebene bietet einen Überblick über aktuelle und vergangene Ereignisse.

Der folgende Screenshot zeigt ein Beispiel für eine Veranstaltungsseite mit einem einzelnen laufenden Ereignis. Dieses aktive Ereignis wird auch im linken Navigationsbereich gekennzeichnet.



The screenshot displays the AWS Shield Advanced console interface. On the left, a navigation sidebar is visible under the heading 'WAF & Shield'. The 'AWS Shield' section is expanded, and 'Events' is highlighted with a red notification badge containing the number '1'. The main content area shows the 'Shield > Events' page. At the top, there is a heading 'Events' followed by a message: 'The following are the events detected by AWS Shield Advanced. For assistance mitigating current events contact the AWS DDoS Response Team'. Below this is a table with the following data:

AWS resource	Current status	Attack vectors	Start time	Duration
E1 - Cloudfront distribution	Mitigation in-progress	UDP traffic	Sep 16th 2020, 2:43:00 pm SAST	6 minutes

Shield Advanced kann je nach Art des Datenverkehrs und den von Ihnen konfigurierten Schutzmaßnahmen auch automatisch Abhilfemaßnahmen gegen Angriffe ergreifen. Diese

Abhilfemaßnahmen können Ihre Ressource davor schützen, übermäßigen Datenverkehr oder Datenverkehr zu empfangen, der einer bekannten DDoS-Angriffssignatur entspricht.

Der folgende Screenshot zeigt ein Beispiel für Ereignisse, bei denen alle Ereignisse durch Shield Advanced gemildert wurden oder von selbst abgeklungen sind.

AWS resource	Current status	Attack vectors	Start time	Duration
- Application load balancer	Identified (subsided)	Request flood	Apr 12th 2022, 8:17:00 am PDT	11 minutes
- Application load balancer	Identified (subsided)	Request flood	Apr 11th 2022, 9:58:00 pm PDT	8 minutes
- Application load balancer	Identified (subsided)	Request flood	Apr 11th 2022, 7:11:00 pm PDT	12 minutes
- Application load balancer	Identified (subsided)	Request flood	Apr 8th 2022, 11:04:00 am PDT	43 minutes
- Protection group	Identified (subsided)	Request flood	Nov 29th 2021, 5:27:00 pm PST	an hour
Cloudfront distribution	Identified (subsided)	Request flood	Nov 29th 2021, 5:26:00 pm PST	an hour
Protection group	Identified (subsided)	Request flood	Nov 29th 2021, 10:38:00 am PST	33 minutes
Cloudfront distribution	Identified (subsided)	Request flood	Nov 29th 2021, 10:37:00 am PST	33 minutes
- Cloudfront distribution	Mitigated	SYN flood	Sep 15th 2021, 3:00:00 am PDT	13 hours

Schützen Sie Ihre Ressourcen vor einem Ereignis

Verbessern Sie die Genauigkeit der Ereigniserkennung, indem Sie Ressourcen mit Shield Advanced schützen, während sie den normalen erwarteten Datenverkehr empfangen, bevor sie einem DDoS-Angriff ausgesetzt sind.

Um Ereignisse für eine geschützte Ressource korrekt melden zu können, muss Shield Advanced zunächst eine Basislinie der erwarteten Datenverkehrsmuster für diese Ressource erstellen.

- Shield Advanced meldet Ereignisse auf Infrastrukturebene für Ressourcen, nachdem sie mindestens 15 Minuten lang geschützt wurden.
- Shield Advanced meldet Ereignisse auf Webanwendungsebene für Ressourcen, nachdem sie mindestens 24 Stunden lang geschützt wurden. Die Genauigkeit der Erkennung von Ereignissen auf Anwendungsebene ist am besten, wenn Shield Advanced den erwarteten Verkehr 30 Tage lang beobachtet hat.

Um auf Ereignisinformationen in der AWS Shield Konsole zuzugreifen

1. Melden Sie sich bei der AWS WAF & Shield-Konsole an AWS Management Console und öffnen Sie sie unter <https://console.aws.amazon.com/wafv2/>.

2. Wählen Sie im AWS Shield Navigationsbereich Ereignisse aus. In der Konsole wird die Seite Ereignisse angezeigt.
3. Auf der Seite Ereignisse können Sie ein beliebiges Ereignis in der Liste auswählen, um zusätzliche Übersichtsinformationen und Details zu dem Ereignis anzuzeigen.

Themen

- [AWS Shield Advanced Zusammenfassungen der Ereignisse](#)
- [AWS Shield Advanced Einzelheiten zur Veranstaltung](#)

AWS Shield Advanced Zusammenfassungen der Ereignisse

Sie können die Zusammenfassung und die Detailinformationen zu einem Ereignis auf der Konsolenseite des Ereignisses einsehen. Um die Seite für ein Ereignis zu öffnen, wählen Sie den Namen der AWS Ressource aus der Liste der Events-Seiten aus.

Der folgende Screenshot zeigt ein Beispiel für eine Ereigniszusammenfassung für ein Ereignis auf Netzwerkebene.

The screenshot displays the AWS Shield Advanced console interface. At the top, there is a breadcrumb navigation path: "Shield > Events > [Redacted]". Below this, the "Event summary" section is visible. It is divided into two columns of information:

Field	Value
AWS resource	arn:aws:cloudfront::[Redacted]:distribution/[Redacted]
Protection	FMManagedShieldProtection [Redacted]
Attack vectors	UDP traffic
Automatic application layer DDoS mitigation	Not applicable
Start time	Jan 13th 2022, 2:06:00 am PST
Network layer automatic mitigation	Enabled
End time	Jan 13th 2022, 2:11:00 am PST
Status	Mitigated

Die zusammenfassenden Informationen auf der Ereignisseite umfassen Folgendes.

- **Aktueller Status** — Werte, die den Status des Ereignisses und die Aktionen angeben, die Shield Advanced für das Ereignis ergriffen hat. Statuswerte gelten für Ereignisse auf Infrastrukturebene (Schicht 3 oder 4) und Anwendungsebene (Schicht 7).
 - **Identifiziert (fortlaufend) und Identifiziert (abgeklungen)** — Diese deuten darauf hin, dass Shield Advanced ein Ereignis erkannt, aber bisher keine Maßnahmen ergriffen hat. Identifiziert (abgeklungen) bedeutet, dass der verdächtige Verkehr, den Shield erkannt hat, ohne Eingreifen gestoppt wurde.
 - **Schadensbegrenzung im Gange und Abhilfe** — Diese Angaben weisen darauf hin, dass Shield Advanced ein Ereignis erkannt und entsprechende Maßnahmen ergriffen hat. Mitigation wird auch verwendet, wenn es sich bei der Zielressource um eine von Amazon CloudFront Distribution oder Amazon Route 53 gehostete Zone handelt, die über eigene automatische Inline-Mitigations verfügt.
- **Angriffsvektoren** — DDoS-Angriffsvektoren wie TCP-SYN-Floods und Shield Advanced-Erkennungsheuristiken wie Request Flood. Dies können Indikatoren für einen DDoS-Angriff sein.
- **Startzeit** — Datum und Uhrzeit, an dem der erste anomale Verkehrsdatenpunkt erkannt wurde.
- **Dauer oder Endzeit** — Gibt die Zeit an, die zwischen der Startzeit des Ereignisses und dem letzten beobachteten anomalen Datenpunkt verstrichen ist, den Shield Advanced beobachtet hat. Während ein Ereignis andauert, werden diese Werte weiter steigen.
- **Schutz** — Benennt den Shield Advanced-Schutz, der mit der Ressource verknüpft ist, und stellt einen Link zu seiner Schutzseite bereit. Dieser ist auf der Seite des jeweiligen Ereignisses verfügbar.
- **Automatische DDoS-Abwehr auf Anwendungsebene** — Wird für den Schutz auf Anwendungsebene verwendet, um anzugeben, ob die automatische Shield Advanced-DDoS-Abwehr auf Anwendungsebene für die Ressource aktiviert ist. Wenn sie aktiviert ist, bietet sie einen Link, über den Sie auf die Konfiguration zugreifen und sie verwalten können. Dieser ist auf der Seite der einzelnen Veranstaltung verfügbar.
- **Automatische Risikominderung auf Netzwerkebene** — Gibt an, ob für die Ressource eine automatische Abwehr auf Netzwerkebene erfolgt. Wenn eine Ressource über eine Komponente auf Netzwerkschicht verfügt, wird diese aktiviert. Diese Informationen sind auf der Seite der einzelnen Veranstaltung verfügbar.

Für Ressourcen, die häufig angegriffen werden, kann Shield nach dem Abklingen des übermäßigen Datenverkehrs Schutzmaßnahmen ergreifen, um weitere wiederkehrende Ereignisse zu verhindern.

Note

Sie können über den API-Vorgang auch auf Ereigniszusammenfassungen für geschützte Ressourcen zugreifen. AWS Shield [ListAttacks](#)

AWS Shield Advanced Einzelheiten zur Veranstaltung

Im unteren Bereich der Konsolenseite für das Ereignis finden Sie Einzelheiten zur Erkennung und Abwehr eines Ereignisses sowie zu den wichtigsten Mitwirkenden. Dieser Abschnitt kann eine Mischung aus legitimem und potenziell unerwünschtem Datenverkehr enthalten und kann sowohl Datenverkehr darstellen, der an Ihre geschützte Ressource weitergeleitet wurde, als auch Datenverkehr, der durch Shield-Schutzmaßnahmen blockiert wurde.

- **Erkennung und Abwehr** — Bietet Informationen über das beobachtete Ereignis und alle getroffenen Gegenmaßnahmen. Informationen zur Abwehr von Ereignissen finden Sie unter [Reagieren auf DDoS-Ereignisse](#)
- **Wichtigste Mitwirkende** — Kategorisiert den Traffic, der an der Veranstaltung beteiligt ist, und listet die wichtigsten Verkehrsquellen auf, die Shield für jede Kategorie identifiziert hat. Verwenden Sie bei Ereignissen auf Anwendungsebene die Informationen der wichtigsten Mitwirkenden, um sich einen allgemeinen Überblick über die Art eines Ereignisses zu verschaffen. Verwenden Sie jedoch die AWS WAF Protokolle für Ihre Sicherheitsentscheidungen. Weitere Informationen finden Sie in den folgenden Abschnitten.

Ihre Ereignisinformationen in der Shield Advanced-Konsole basieren auf Shield Advanced-Metriken. Informationen zu Shield Advanced-Metriken finden Sie unter [AWS Shield Advanced Metriken](#)

Risikominderungsmetriken für Amazon CloudFront - oder Amazon Route 53-Ressourcen sind nicht enthalten, da diese Services durch ein Abwehrsystem geschützt sind, das immer aktiviert ist und keine Abhilfemaßnahmen für einzelne Ressourcen erfordert.

Die einzelnen Abschnitte variieren je nachdem, ob sich die Informationen auf ein Ereignis auf der Infrastrukturebene oder auf Anwendungsebene beziehen.

Details zum Ereignis auf Anwendungsebene

Im unteren Bereich der Konsolenseite für das Ereignis finden Sie Einzelheiten zur Erkennung und Abwehr eines Ereignisses auf Anwendungsebene sowie zu den wichtigsten Mitwirkenden. Dieser Abschnitt kann eine Mischung aus legitimem und potenziell unerwünschtem Datenverkehr enthalten

und kann sowohl Datenverkehr darstellen, der an Ihre geschützte Ressource weitergeleitet wurde, als auch Datenverkehr, der durch Shield Advanced-Mitigations blockiert wurde.

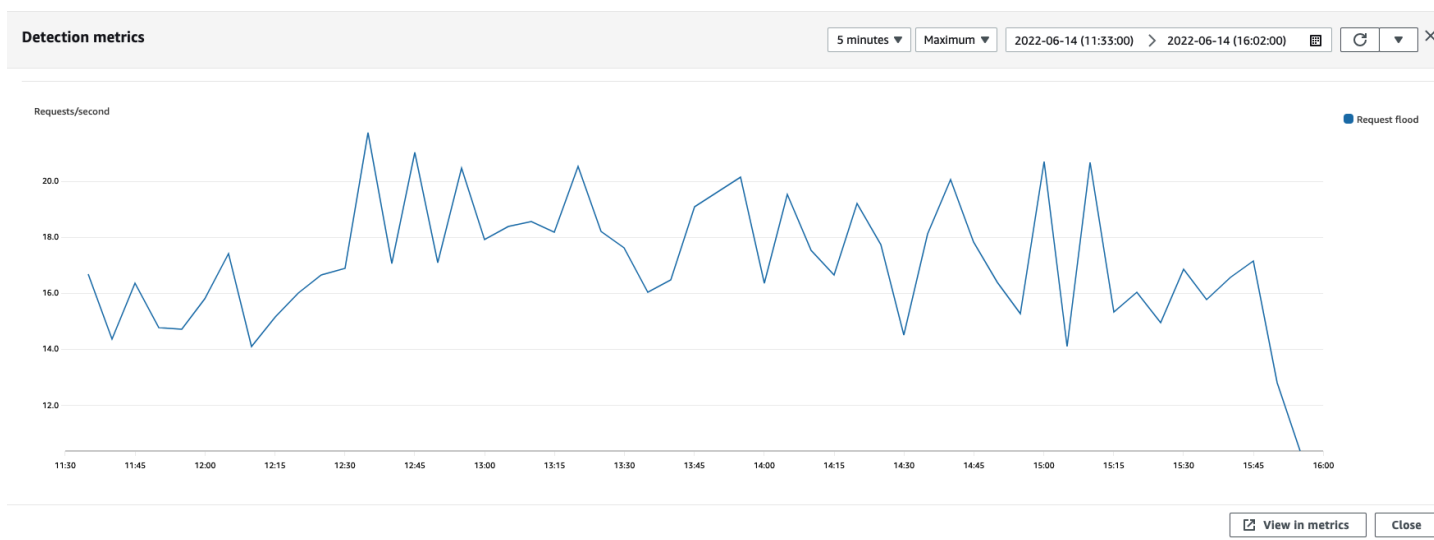
Die Schadensbegrenzungsdetails beziehen sich auf alle Regeln in der Web-ACL, die mit der Ressource verknüpft sind, einschließlich Regeln, die speziell als Reaktion auf einen Angriff eingesetzt werden, und ratenbasierte Regeln, die in der Web-ACL definiert sind. Wenn Sie die automatische DDoS-Abwehr auf Anwendungsebene für eine Anwendung aktivieren, enthalten die Abhilfemetriken Metriken für diese zusätzlichen Regeln. Informationen zu diesen Schutzmaßnahmen auf Anwendungsebene finden Sie unter [AWS Shield Advanced Schutzmaßnahmen auf Anwendungsebene \(Schicht 7\)](#)

Erkennung und Schadensbegrenzung

Für ein Ereignis auf Anwendungsebene (Schicht 7) werden auf der Registerkarte Erkennung und Schadensbegrenzung Erkennungsmetriken angezeigt, die auf Informationen aus den AWS WAF Protokollen basieren. Die Metriken zur Schadensbegrenzung basieren auf AWS WAF Regeln in der zugehörigen Web-ACL, die so konfiguriert sind, dass unerwünschter Datenverkehr blockiert wird.

Für CloudFront Amazon-Distributionen können Sie Shield Advanced so konfigurieren, dass automatische Abhilfemaßnahmen für Sie angewendet werden. Für alle Ressourcen auf Anwendungsebene können Sie Ihre eigenen Abwehrregeln in Ihrer Web-ACL definieren und das Shield Response Team (SRT) um Hilfe bitten. Weitere Informationen zu diesen Optionen finden Sie unter [Reagieren auf DDoS-Ereignisse](#).

Der folgende Screenshot zeigt ein Beispiel für die Erkennungsmetriken für ein Ereignis auf Anwendungsebene, das nach einigen Stunden wieder abgeklungen ist.



Event-Traffic, der nachlässt, bevor eine Schadensbegrenzungsregel wirksam wird, wird in den Risikometriken nicht berücksichtigt. Dies kann zu einem Unterschied zwischen dem in den Erkennungsdiagrammen angezeigten Webanforderungs-Traffic und den in den Risikominderungsdiagrammen angezeigten Zulassen und Blockierungs-Metriken führen.

Die wichtigsten Mitwirkenden

Auf der Registerkarte Wichtigste Mitwirkende für Ereignisse auf Anwendungsebene werden die fünf wichtigsten Mitwirkenden angezeigt, die Shield für das Ereignis identifiziert hat, basierend auf den abgerufenen AWS WAF Protokollen. Shield kategorisiert die Informationen der wichtigsten Mitwirkenden nach Dimensionen wie Quell-IP, Quellland und Ziel-URL.

Note

Die genauesten Informationen über den Datenverkehr, der zu einem Ereignis auf Anwendungsebene beiträgt, finden Sie in den AWS WAF Protokollen.

Verwenden Sie die Informationen der wichtigsten Mitwirkenden der Shield-Anwendungsebene nur, um sich einen allgemeinen Überblick über die Art eines Angriffs zu verschaffen, und stützen Sie Ihre Sicherheitsentscheidungen nicht darauf. Bei Ereignissen auf Anwendungsebene sind die AWS WAF Protokolle die beste Informationsquelle, um die Verursacher eines Angriffs zu verstehen und Ihre Abwehrstrategien zu entwickeln.

Die Informationen der wichtigsten Mitwirkenden von Shield spiegeln nicht immer vollständig die Daten in den AWS WAF Protokollen wider. Bei der Aufnahme der Protokolle räumt Shield der Reduzierung der Auswirkungen auf die Systemleistung Vorrang vor dem Abrufen des vollständigen Datensatzes aus den Protokollen ein. Dies kann zu einem Verlust der Granularität der Daten führen, die Shield zur Analyse zur Verfügung stehen. In den meisten Fällen ist der Großteil der Informationen verfügbar, aber es ist möglich, dass die Daten der wichtigsten Mitwirkenden bei jedem Angriff bis zu einem gewissen Grad verzerrt werden.

Der folgende Screenshot zeigt ein Beispiel für eine Registerkarte mit den wichtigsten Mitwirkenden für ein Ereignis auf Anwendungsebene.

Detection and mitigation			Top contributors		
Application			Network		
Top 5 source IP addresses			Top 5 source countries		
Source IP	Total requests	Percentage of traffic	Source country	Total requests	Percentage of traffic
34.203.230.194	4392300	65.42%	US	6714171	100.00%
23.22.196.86	1282506	19.10%			
3.83.54.134	1039365	15.48%			
Top 5 destination URLs			Top 5 user agents		
Destination URL	Total requests	Percentage of traffic	Source user agent		
/	4425825	65.92%	Mozilla/5.0 (Macintosh; Intel Mac OS X 12_0_1) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Safari/605.1.15		
/[REDACTED].js	397737	5.92%	python/gevent-http-client-1.5.3		
/styles.css	381830	5.69%			
/runtime/[REDACTED].js	378136	5.63%			
/assets/public/images/[REDACTED].jpg	202612	3.02%			

Die Informationen der Mitwirkenden basieren auf Anfragen sowohl für legitimen als auch für potenziell unerwünschten Datenverkehr. Bei Ereignissen mit größerem Volumen und bei Ereignissen, bei denen die Anforderungsquellen nicht weit verbreitet sind, ist die Wahrscheinlichkeit höher, dass die wichtigsten Mitwirkenden identifiziert werden können. Ein stark verteilter Angriff kann eine beliebige Anzahl von Quellen haben, was es schwierig macht, die Hauptverursacher des Angriffs zu identifizieren. Wenn Shield Advanced keine wesentlichen Mitwirkenden für eine bestimmte Kategorie identifiziert, werden die Daten als nicht verfügbar angezeigt.

Einzelheiten zu Ereignissen auf Infrastrukturebene

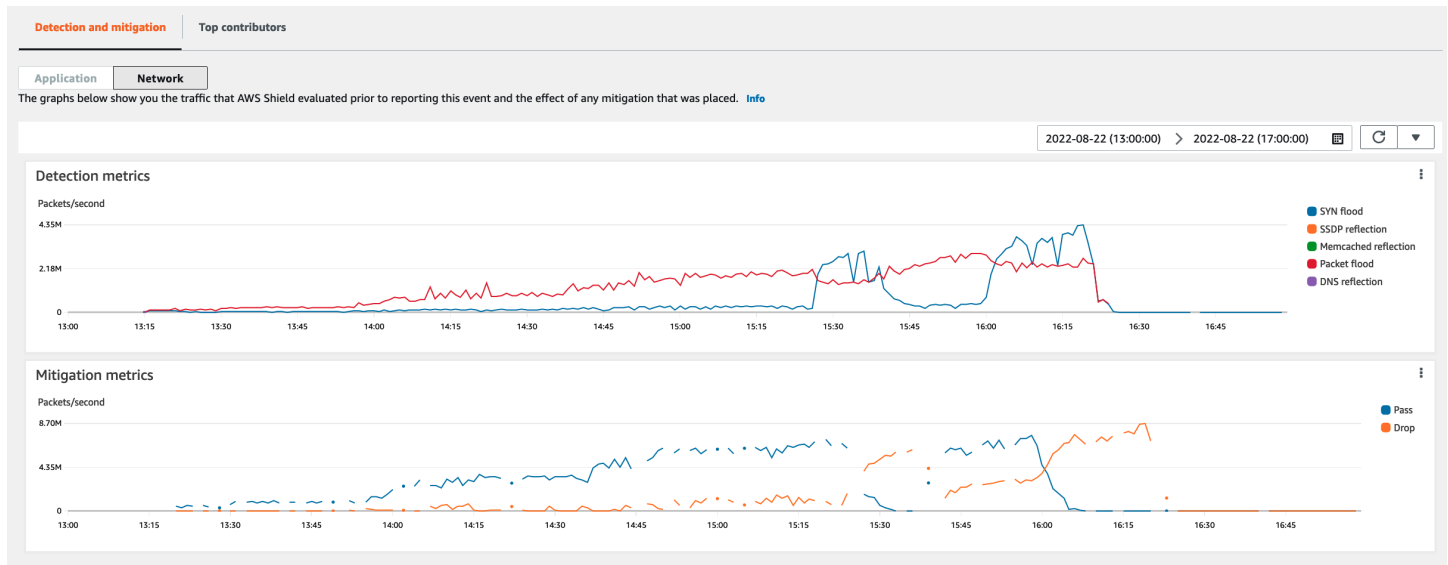
Im unteren Bereich der Konsolenseite für das Ereignis finden Sie Einzelheiten zur Erkennung und Abwehr eines Ereignisses auf Infrastrukturebene sowie zu den wichtigsten Mitwirkenden. Dieser Abschnitt kann eine Mischung aus legitimem und potenziell unerwünschtem Datenverkehr enthalten und kann sowohl Datenverkehr darstellen, der an Ihre geschützte Ressource weitergeleitet wurde, als auch Datenverkehr, der durch Shield-Schutzmaßnahmen blockiert wurde.

Erkennung und Abwehr

Für ein Ereignis auf der Infrastrukturebene (Schicht 3 oder 4) werden auf der Registerkarte Erkennung und Schadensbegrenzung Erkennungsmetriken angezeigt, die auf Stichproben von Netzwerkströmen basieren, sowie Risikominderungsmetriken, die auf dem von den Minderungssystemen beobachteten Datenverkehr basieren. Risikominderungsmetriken sind eine genauere Messung des Datenverkehrs, der in Ihre Ressource fließt.

Shield erstellt automatisch eine Abwehr für die geschützten Ressourcentypen Elastic IP (EIP), Classic Load Balancer (CLB), Application Load Balancer (ALB) und Standard Accelerator. AWS Global Accelerator Abhilfemetriken für EIP-Adressen und AWS Global Accelerator Standardbeschleuniger geben die Anzahl der übergebenen und verworfenen Pakete an.

Der folgende Screenshot zeigt ein Beispiel für die Registerkarte Erkennung und Schadensbegrenzung für ein Ereignis auf Infrastrukturebene.

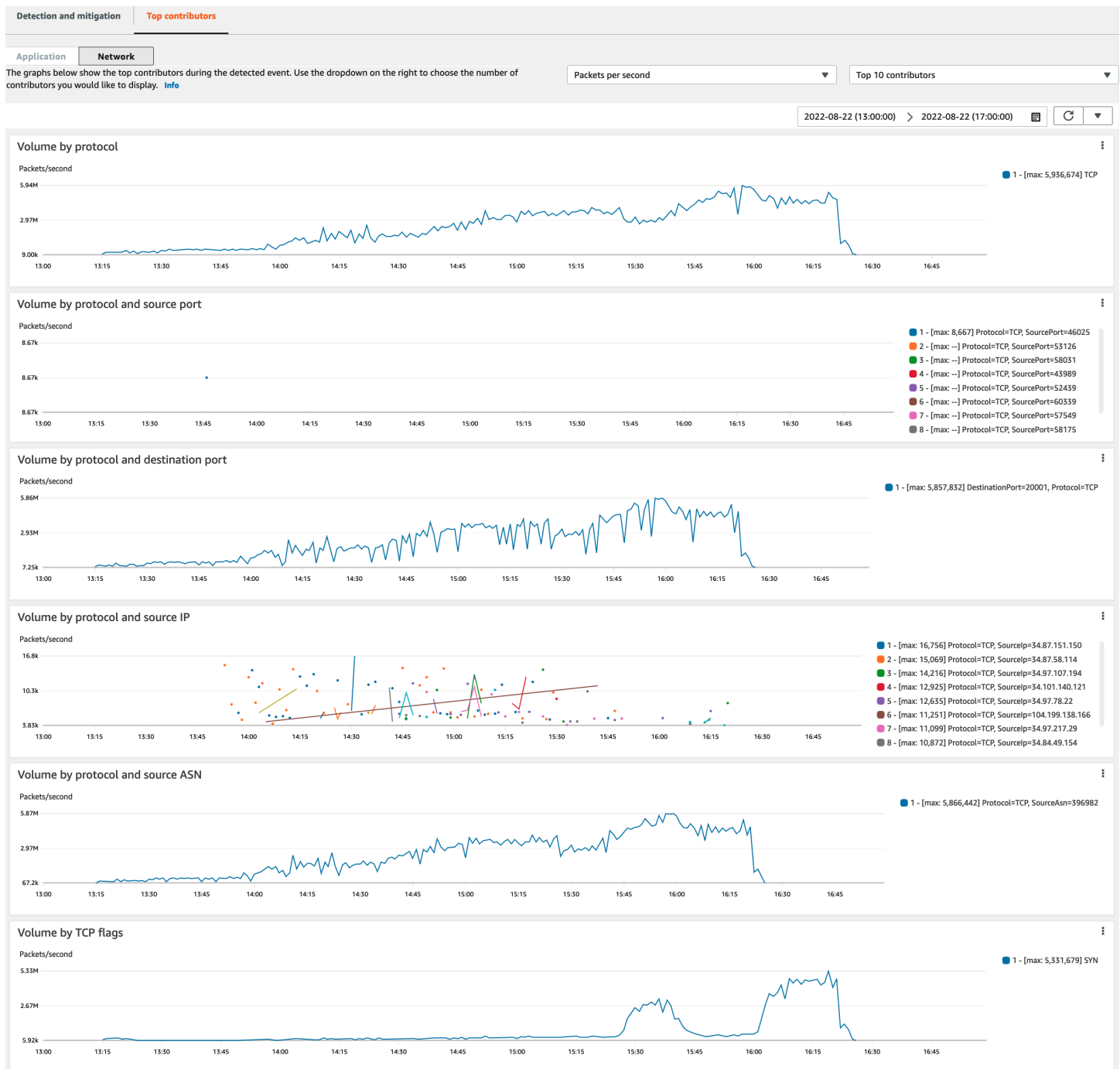


Event-Traffic, der nachlässt, bevor Shield eine Schadensbegrenzung einleitet, wird in den Risikominderungsmetriken nicht berücksichtigt. Dies kann zu einem Unterschied zwischen dem in den Erkennungsdiagrammen angezeigten Verkehr und den Pass-and-Drop-Metriken in den Risikominderungsdiagrammen führen.

Die wichtigsten Mitwirkenden

Auf der Registerkarte mit den wichtigsten Mitwirkenden für Ereignisse auf Infrastrukturebene sind Metriken für bis zu 100 Hauptverursacher in verschiedenen Verkehrsdimensionen aufgeführt. Zu den Details gehören Eigenschaften der Netzwerkschicht für jede Dimension, bei der mindestens fünf signifikante Verkehrsquellen identifiziert werden konnten. Beispiele für Verkehrsquellen sind Quell-IP und Quell-ASN.

Der folgende Screenshot zeigt ein Beispiel für eine Registerkarte mit den wichtigsten Mitwirkenden für ein Ereignis auf Infrastrukturebene.



Die Metriken der Mitwirkenden basieren auf Stichproben von Netzwerkströmen sowohl für legitimen als auch für potenziell unerwünschten Datenverkehr. Bei Ereignissen mit größerem Volumen und Ereignissen, bei denen die Datenverkehrsquellen nicht stark verteilt sind, ist die Wahrscheinlichkeit höher, dass die Hauptverursacher identifiziert werden können. Ein stark verteilter Angriff kann eine beliebige Anzahl von Quellen haben, was es schwierig macht, die Hauptverursacher des Angriffs zu identifizieren. Wenn Shield keine wesentlichen Mitwirkenden für eine bestimmte Metrik oder Kategorie identifiziert, werden die Daten als nicht verfügbar angezeigt.

Bei einem DDoS-Angriff auf Infrastrukturebene können Datenverkehrsquellen gefälscht oder widergespiegelt werden. Eine gefälschte Quelle wird vom Angreifer absichtlich gefälscht. Eine reflektierte Quelle ist die eigentliche Quelle des erkannten Datenverkehrs, aber sie ist nicht bereit, sich an dem Angriff zu beteiligen. Ein Angreifer könnte beispielsweise eine große, verstärkte Flut von Datenverkehr zu einem Ziel erzeugen, indem er den Angriff von Diensten im Internet ableitet, die normalerweise legitim sind. In diesem Fall sind die Quellinformationen möglicherweise gültig, obwohl sie nicht die eigentliche Quelle des Angriffs sind. Diese Faktoren können die Durchführbarkeit von Abhilfemaßnahmen einschränken, die Quellen auf der Grundlage von Paket-Headern blockieren.

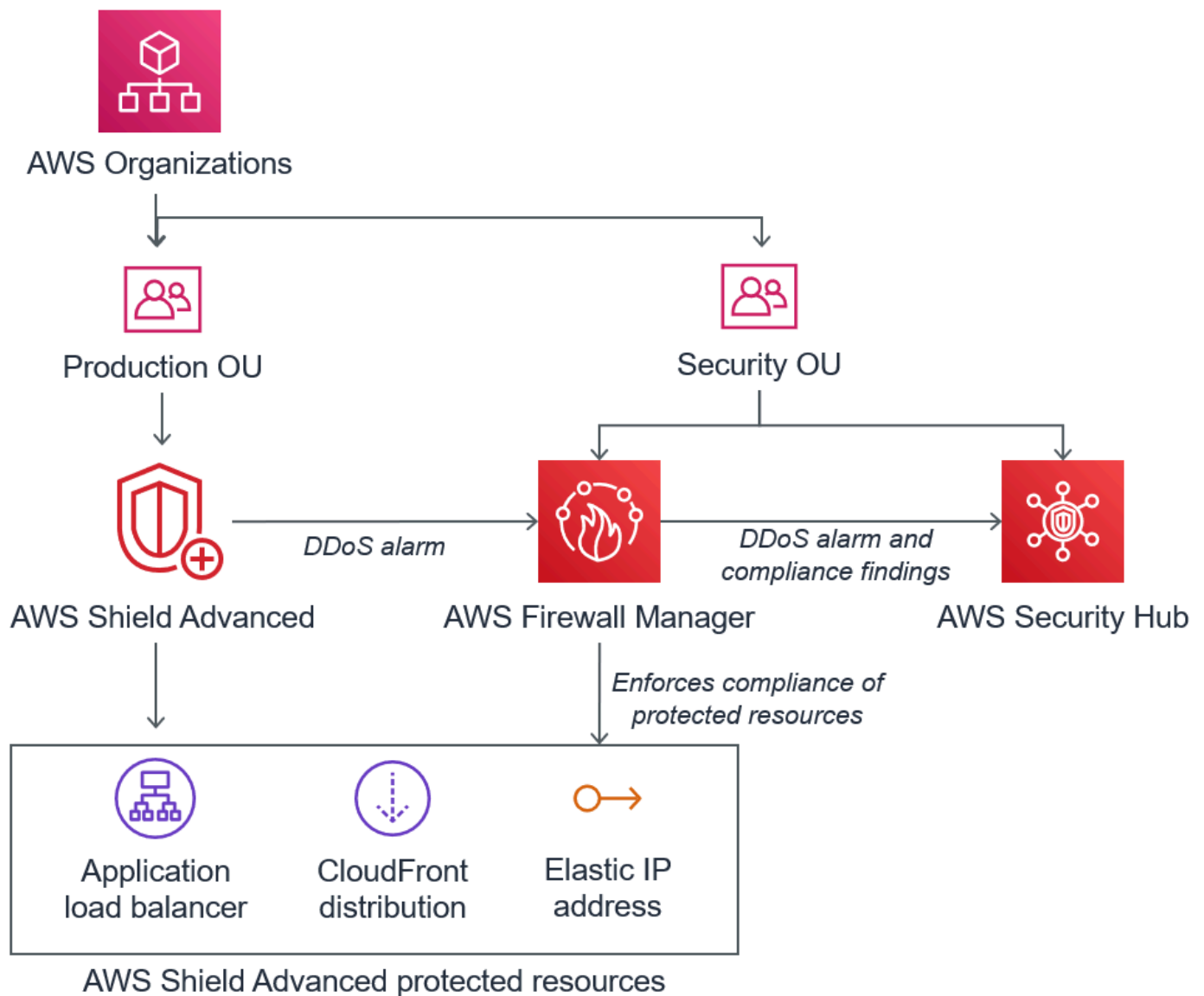
Kontoübergreifende Sichtbarkeit von Ereignissen

Sie können AWS Shield Advanced geschützte Ressourcen AWS Security Hub für mehrere Konten verwenden AWS Firewall Manager und verwalten und überwachen.

Mit Firewall Manager können Sie eine Shield Advanced-Sicherheitsrichtlinie erstellen, die die Einhaltung des DDoS-Schutzes für all Ihre Konten meldet und durchsetzt. Firewall Manager überwacht Ihre geschützten Ressourcen und fügt auch Schutzmaßnahmen für neue Ressourcen hinzu, die in den Geltungsbereich der Shield Advanced-Richtlinie fallen.

Sie können Firewall Manager integrieren, AWS Security Hub um ein einziges Dashboard zu erhalten, das DDoS-Ereignisse meldet, die von Shield Advanced und Firewall Manager-Konformitätsergebnissen erkannt wurden, wenn Firewall Manager eine Ressource identifiziert, die nicht Ihren Shield Advanced-Sicherheitsrichtlinien entspricht.

Die folgende Abbildung zeigt eine typische Architektur für die Überwachung geschützter Shield Advanced-Ressourcen mit Firewall Manager und Security Hub.



Wenn Sie Firewall Manager in Security Hub integrieren, können Sie Sicherheitsergebnisse zusammen mit anderen Warnmeldungen und Compliance-Statusinformationen für die Anwendungen, auf denen Sie laufen, an einem zentralen Ort einsehen AWS.

Der folgende Screenshot zeigt die Informationen, die Sie für ein Shield Advanced-Ereignis in der Security Hub Hub-Konsole sehen können, wenn Sie über eine solche Integration verfügen.

Security Hub > Findings

Findings

A finding is a security issue or a failed security check.

Actions Change workflow status Create insight

Shield Advanced detected attack against monitored resource

Finding ID: arn:aws:insus-east-1:3502:49:finding/842e6137-a20a-44f0-9027-dd2233746280/loadbalancer/app/loadbalancer-3/dca87d7482d89b7f

• INFORMATIONAL

Shield Advanced detected an attack on the protected resource arn:aws:elasticloadbalancing:us-east-1:3502:49:loadbalancer/app/loadbalancer-3/dca87d7482d89b7f.

Workflow status: New

RECORD STATE: ACTIVE

Set by the finding provider

Severity	Workflow status	Company	Product	Title	Resource ID	Resource type	Status
• INFORMATIONAL	NEW	AWS	Firewall Manager	Shield Advanced detected attack against monitored resource	arn:aws:elasticloadbalancing:us-east-1:3502:49:loadbalancer/app/loadbalancer-3/dca87d7482d89b7f	Other	

AWS account ID: 3502 49

Severity (original): 0

Severity (normalized): 0

Updated at: 2020-07-15T14:55:36.718Z

Severity label: INFORMATIONAL

Source URL: https://console.aws.amazon.com/wafv2/fms?region=us-east-1#/securitypolicies-compliance/842e6137-a20a-44f0-9027-dd2233746280/3502:49

Types and Related Findings

Resources

Remediation

Enable Firewall Manager policy remediation.

Wie Sie Firewall Manager und Security Hub mit Shield Advanced integrieren können, um die Ereignis- und Compliance-Überwachung Ihrer geschützten Konten zu [zentralisieren, finden Sie im AWS Sicherheitsblog Zentrale Überwachung für DDoS-Ereignisse einrichten und nicht konforme Ressourcen automatisch korrigieren.](#)

Reagieren auf DDoS-Ereignisse

AWS wehrt Distributed-Denial-of-Service-Angriffe (DDoS) auf Netzwerk- und Transportebene (Layer 3 und Layer 4) automatisch ab. Wenn Sie Shield Advanced zum Schutz Ihrer Amazon EC2 EC2-Instances verwenden, verteilt Shield Advanced während eines Angriffs automatisch Ihre Amazon VPC-Netzwerk-ACLs an der Netzwerkgrenze. AWS Dadurch kann Shield Advanced Schutz vor größeren DDoS-Ereignissen bieten. Weitere Informationen zu Netzwerk-ACLs finden Sie unter [Network ACLs](#).

Bei DDoS-Angriffen auf Anwendungsebene (Schicht 7) wird AWS versucht, AWS Shield Advanced Kunden durch CloudWatch Alarme zu erkennen und zu benachrichtigen. Standardmäßig werden Abhilfemaßnahmen nicht automatisch angewendet, um zu verhindern, dass versehentlich gültiger Benutzerverkehr blockiert wird.

Für Ressourcen auf Anwendungsebene (Schicht 7) stehen Ihnen die folgenden Optionen zur Verfügung, um auf einen Angriff zu reagieren.

- Stellen Sie Ihre eigenen Abhilfemaßnahmen bereit — Sie können den Angriff selbst untersuchen und abwehren. Weitere Informationen finden Sie unter [Manuelles Abwehren eines DDoS-Angriffs auf Anwendungsebene](#).
- Support kontaktieren — Wenn Sie ein Shield Advanced-Kunde sind, können Sie sich an das [AWS Support Center](#) wenden, um Hilfe bei Abhilfemaßnahmen zu erhalten. Kritische und dringende Fälle werden direkt an DDoS-Experten weitergeleitet. Weitere Informationen finden Sie unter [Kontaktaufnahme mit dem Support Center während eines DDoS-Angriffs auf Anwendungsebene](#).

Darüber hinaus können Sie, bevor ein Angriff stattfindet, proaktiv die folgenden Abhilfemaßnahmen aktivieren:

- Automatische Abhilfemaßnahmen Amazon CloudFront Amazon-Distributionen — Mit dieser Option definiert und verwaltet Shield Advanced Regeln zur Schadensbegrenzung für Sie in Ihrer Web-ACL. Informationen zur automatischen Schadensbegrenzung auf Anwendungsebene finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#)
- Proaktives Eingreifen — Wenn ein umfangreicher Angriff auf Anwendungsebene gegen eine Ihrer Anwendungen AWS Shield Advanced erkannt wird, kann das SRT Sie proaktiv kontaktieren. Das SRT analysiert das DDoS-Ereignis und sorgt für Gegenmaßnahmen. AWS WAF Das SRT kontaktiert Sie und kann mit Ihrer Zustimmung die Regeln anwenden. AWS WAF Weitere Informationen zu dieser Option finden Sie unter [Konfiguration von proaktivem Engagement](#).

Kontaktaufnahme mit dem Support Center während eines DDoS-Angriffs auf Anwendungsebene

Wenn Sie ein AWS Shield Advanced Kunde sind, können Sie sich an das [AWS Support Center](#) wenden, um Hilfe bei der Abwehr zu erhalten. Kritische und dringende Fälle werden direkt an DDoS-Experten weitergeleitet. Mit AWS Shield Advanced können komplexe Fälle an das AWS Shield Response Team (SRT) weitergeleitet werden, das über umfangreiche Erfahrung im Schutz AWS von Amazon.com und seinen Tochtergesellschaften verfügt. Weitere Informationen zum SRT finden Sie unter [Unterstützung durch das Shield Response Team \(SRT\)](#)

Um Support vom Shield Response Team (SRT) zu erhalten, wenden Sie sich an das [AWS Support Center](#). Die Reaktionszeit für Ihren Fall hängt vom ausgewählten Schweregrad und den Reaktionszeiten ab, die auf der Seite [AWS Support Pläne](#) dokumentiert sind.

Wählen Sie die folgenden Optionen:

- Falltyp: Technischer Support
- Service: Distributed Denial of Service (DDoS)
- Kategorie: Eingehend an AWS
- Schweregrad: Wählen Sie eine geeignete Option

Erläutern Sie im Gespräch mit unserem Vertreter, dass Sie ein AWS Shield Advanced Kunde sind, der von einem möglichen DDoS-Angriff betroffen ist. Unsere Mitarbeiter leiten Ihren Anruf an die entsprechenden DDoS-Experten weiter. Wenn Sie beim [AWS Support Center](#) einen Fall über den Servicetyp Distributed Denial of Service (DDoS) eröffnen, können Sie per Chat oder Telefon direkt mit einem DDoS-Experten sprechen. DDoS-Supporttechniker können Ihnen bei der Identifizierung von Angriffen helfen, Verbesserungen an Ihrer AWS Architektur empfehlen und Sie bei der Nutzung von AWS Diensten zur Abwehr von DDoS-Angriffen beraten.

Bei Angriffen auf Anwendungsebene kann Ihnen das SRT bei der Analyse verdächtiger Aktivitäten helfen. Wenn Sie die automatische Abwehr für Ihre Ressource aktiviert haben, kann das SRT die Abhilfemaßnahmen überprüfen, die Shield Advanced automatisch gegen den Angriff einleitet. In jedem Fall kann Ihnen das SRT dabei helfen, das Problem zu überprüfen und zu beheben. Die vom SRT empfohlenen Maßnahmen erfordern häufig, dass das SRT AWS WAF Web-Zugriffskontrolllisten (Web-ACLs) in Ihrem Konto erstellt oder aktualisiert. Für diese Arbeit benötigt das SRT Ihre Zustimmung.

Important

Wir empfehlen, dass Sie im Rahmen der Aktivierung die unter beschriebenen Schritte befolgen AWS Shield Advanced, [Konfiguration des Zugriffs für das Shield Response Team \(SRT\)](#) um dem SRT proaktiv die Berechtigungen zu erteilen, die es benötigt, um Sie bei einem Angriff zu unterstützen. Die frühzeitige Zustimmung verhindert Verzögerungen im Falle eines tatsächlichen Angriffs.

Das SRT hilft Ihnen bei der Triage des DDoS-Angriffs, um Angriffssignaturen und -muster zu identifizieren. Mit Ihrer Zustimmung erstellt und implementiert das SRT AWS WAF Regeln zur Abwehr des Angriffs.

Sie können sich auch vor oder während eines möglichen Angriffs an das SRT wenden, um Abhilfemaßnahmen zu überprüfen und maßgeschneiderte Abhilfemaßnahmen zu entwickeln und einzusetzen. Wenn Sie beispielsweise eine Webanwendung ausführen und nur die Ports 80 und 443

geöffnet haben müssen, können Sie mit dem SRT eine Web-ACL so vorkonfigurieren, dass nur die Ports 80 und 443 „zugelassen“ werden.

Sie autorisieren und kontaktieren das SRT auf Kontoebene. Das heißt, wenn Sie Shield Advanced innerhalb einer Firewall Manager Shield Advanced-Richtlinie verwenden, muss sich der Kontoinhaber, nicht der Firewall Manager Manager-Administrator, an das SRT wenden, um Support zu erhalten. Der Firewall Manager Manager-Administrator kann das SRT nur für Konten kontaktieren, die er besitzt.

Manuelles Abwehren eines DDoS-Angriffs auf Anwendungsebene

Wenn Sie feststellen, dass die Aktivität auf der Ereignisseite für Ihre Ressource einen DDoS-Angriff darstellt, können Sie in Ihrer Web-ACL eigene AWS WAF Regeln erstellen, um den Angriff abzuwehren. Dies ist die einzige verfügbare Option, wenn Sie kein Shield Advanced-Kunde sind. AWS WAF ist ohne zusätzliche Kosten AWS Shield Advanced im Preis enthalten. Informationen zum Erstellen von Regeln in Ihrer Web-ACL finden Sie unter [Web-Zugriffskontrolllisten \(Web-ACLs\)](#).

Wenn Sie verwenden AWS Firewall Manager, können Sie Ihre AWS WAF Regeln zu einer Firewall Manager AWS WAF Manager-Richtlinie hinzufügen.

Um einen potenziellen DDoS-Angriff auf Anwendungsebene manuell abzuwehren

1. Erstellen Sie in Ihrer Web-ACL Regelanweisungen mit Kriterien, die dem ungewöhnlichen Verhalten entsprechen. Konfigurieren Sie sie zunächst so, dass übereinstimmende Anfragen gezählt werden. Informationen zur Konfiguration Ihrer Web-ACL und Regelanweisungen finden Sie unter [Auswertung von Web-ACL-Regeln und -Regelgruppen](#) und [Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen](#).

Note

Testen Sie Ihre Regeln immer zuerst, indem Sie zunächst die Regelaktion Count anstelle von verwendenBlock. Wenn Sie sicher sind, dass Ihre neuen Regeln die richtigen Anfragen identifizieren, können Sie sie ändern, um die Anfragen zu blockieren.

2. Überwachen Sie die Anzahl der Anfragen, um festzustellen, ob Sie die entsprechenden Anfragen blockieren möchten. Wenn das Volumen der Anfragen weiterhin ungewöhnlich hoch ist und Sie sicher sind, dass Ihre Regeln die Anfragen erfassen, die das hohe Volumen verursachen, ändern Sie die Regeln in Ihrer Web-ACL, um die Anfragen zu blockieren.

- Überwachen Sie weiterhin die Seite mit den Ereignissen, um sicherzustellen, dass Ihr Datenverkehr so behandelt wird, wie Sie es möchten.

AWS bietet vorkonfigurierte Vorlagen, damit Sie schnell loslegen können. Die Vorlagen enthalten eine Reihe von AWS WAF Regeln, die Sie anpassen und verwenden können, um gängige webbasierte Angriffe zu blockieren. Weitere Informationen finden Sie unter [AWS WAF Security Automations](#).

Eine Gutschrift beantragen in AWS Shield Advanced

Wenn Sie ein Abonnement haben AWS Shield Advanced und von einem DDoS-Angriff betroffen sind, der die Nutzung einer geschützten Shield Advanced-Ressource erhöht, können Sie eine Shield Advanced-Servicegutschrift für Gebühren im Zusammenhang mit der erhöhten Auslastung beantragen, sofern diese nicht durch Shield Advanced gemildert wird.

Gutschriften sind nur für die folgenden Arten von Gebühren verfügbar:

- Shield Advanced ausgehende Datenübertragung
- Amazon CloudFront HTTP/HTTPS-Anfragen
- CloudFront ausgehende Datenübertragung
- Amazon Route 53-Abfragen
- AWS Global Accelerator Standard-Beschleuniger-Datenübertragung
- Load Balancer-Kapazitätseinheiten für Application Load Balancer
- Instanzkosten für geschützte Amazon Elastic Compute Cloud (Amazon EC2) -Instances, die durch eine auto-scaling Skalierungsrichtlinie als Reaktion auf den Angriff erstellt wurden

Voraussetzungen für die Beantragung einer Gutschrift

Um Anspruch auf eine Gutschrift zu haben, müssen Sie vor Beginn des Angriffs Folgendes getan haben:

- Sie müssen den Ressourcen, für die Sie eine Gutschrift beantragen möchten, Shield Advanced-Schutz hinzugefügt haben. Geschützte Ressourcen, die während eines Angriffs hinzugefügt wurden, kommen nicht für den Kostenschutz in Frage.

Note

Die Aktivierung von Shield Advanced auf Ihrem aktiviert AWS-Konto nicht automatisch den Shield Advanced-Schutz für einzelne Ressourcen.

Weitere Informationen zum Schutz von AWS Ressourcen mithilfe von Shield Advanced finden Sie unter [AWS Shield Advanced Schutz für Ressourcen hinzufügen AWS](#).

- Für anwendbare CloudFront und durch Application Load Balancer geschützte Ressourcen müssen Sie eine AWS WAF Web-ACL zugeordnet und eine ratenbasierte Regel in der Web-ACL im Modus implementiert haben. Block Hinweise zu AWS WAF ratenbasierten Regeln finden Sie unter. [Ratenbasierte Regelanweisung](#) Informationen zum Verknüpfen von Web-ACLs mit AWS Ressourcen finden Sie unter. [Web-Zugriffskontrolllisten \(Web-ACLs\)](#)
- Sie müssen die entsprechenden Best Practices in [AWS Best Practices for DDoS Resiliency](#) implementiert haben, um Ihre Anwendung so zu konfigurieren, dass die Kosten bei einem DDoS-Angriff minimiert werden.

Wie beantrage ich einen Kredit

Um Anspruch auf eine Gutschrift zu haben, müssen Sie Ihre Kreditanfrage innerhalb von 15 Tagen unmittelbar nach dem Abrechnungsmonat einreichen, in dem der Angriff stattgefunden hat.

Um eine Gutschrift zu beantragen, reichen Sie einen Rechnungsfall über das [AWS Support Center](#) ein. Fügen Sie Ihrer Anfrage Folgendes bei:

- Die Worte "DDoS-Zugeständnis" in der Betreffzeile
- Datum und Uhrzeit der einzelnen Ereignisse oder Verfügbarkeitsunterbrechungen, für die Sie eine Gutschrift beantragen
- Die AWS Dienste und spezifischen Ressourcen, die betroffen waren

Nachdem Sie eine Anfrage eingereicht haben, überprüft das AWS Shield Response Team (SRT), ob ein DDoS-Angriff stattgefunden hat und, falls ja, ob geschützte Ressourcen skaliert wurden, um den DDoS-Angriff abzuwehren. Es stellt AWS fest, dass die geschützten Ressourcen so skaliert wurden, dass sie den DDoS-Angriff abwehren, und AWS stellt eine Gutschrift für den Teil des Datenverkehrs aus, der AWS feststellt, dass er durch den DDoS-Angriff verursacht wurde. Gutschriften sind für 12 Monate gültig.

Sicherheit bei der Nutzung des AWS Shield Dienstes

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Note

Dieser Abschnitt enthält AWS Standardsicherheitsrichtlinien für Ihre Nutzung des AWS Shield Dienstes und seiner AWS Ressourcen, wie z. B. den erweiterten Schutz von Shield. Informationen zum Schutz Ihrer AWS Ressourcen mit Shield und Shield Advanced finden Sie im Rest des AWS Shield Handbuchs.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Die Wirksamkeit unserer Sicherheitsfunktionen wird regelmäßig von externen Prüfern im Rahmen des [AWS -Compliance-Programms getestet und überprüft](#). Weitere Informationen zu den Compliance-Programmen, die für Shield gelten, finden Sie unter [AWS Services in Scope by Compliance Program](#).
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. In Ihre Verantwortung fallen außerdem weitere Faktoren, wie z. B. die Vertraulichkeit der Daten, die Anforderungen Ihrer Organisation sowie geltende Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Shield anwenden können. In den folgenden Themen erfahren Sie, wie Sie Shield konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre Shield-Ressourcen zu überwachen und zu sichern.

Themen

- [Datenschutz in Shield](#)
- [Identitäts- und Zugriffsmanagement für AWS Shield](#)
- [Protokollierung und Überwachung in Shield](#)

- [Konformitätsvalidierung für Shield](#)
- [Resilienz in Shield](#)
- [Sicherheit der Infrastruktur in AWS Shield](#)

Datenschutz in Shield

Das [Modell der AWS gemeinsamen Verantwortung](#) und geteilter Verantwortung gilt für den Datenschutz in AWS Shield. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter [Häufig gestellte Fragen zum Datenschutz](#). Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag [AWS -Modell der geteilten Verantwortung und in der DSGVO](#) im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-2](#).

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit

Shield oder anderen AWS-Services über die Konsole AWS CLI, API oder AWS SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Shield-Einheiten — wie Schutzeinrichtungen — werden im Ruhezustand verschlüsselt, außer in bestimmten Regionen, in denen Verschlüsselung nicht verfügbar ist, darunter China (Peking) und China (Ningxia). Eindeutige Verschlüsselungsschlüssel werden für jede Region verwendet.

Identitäts- und Zugriffsmanagement für AWS Shield

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service, den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Shield-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service, das Sie ohne zusätzliche Kosten nutzen können.

Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [Wie AWS Shield funktioniert mit IAM](#)
- [Beispiele für identitätsbasierte Richtlinien für AWS Shield](#)
- [AWS verwaltete Richtlinien für AWS Shield](#)
- [Problembehandlung bei AWS Shield Identität und Zugriff](#)
- [Verwenden von serviceverknüpften Rollen für Shield Advanced](#)

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Shield ausführen.

Dienstbenutzer — Wenn Sie den Shield-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Da Sie für Ihre Arbeit mehr Shield-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits,

welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie in Shield nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unter [Problembehandlung bei AWS Shield Identität und Zugriff](#).

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die Shield-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Shield. Es ist Ihre Aufgabe, zu bestimmen, auf welche Shield-Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Shield verwenden kann, finden Sie unter [Wie AWS Shield funktioniert mit IAM](#).

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Shield zu verwalten. Beispiele für identitätsbasierte Shield-Richtlinien, die Sie in IAM verwenden können, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Shield](#)

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter [So melden Sie sich bei Ihrem an AWS-Konto](#) im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen

Methode, um Anfragen selbst zu [signieren](#), finden Sie im [IAM-Benutzerhandbuch unter AWS API-Anfragen](#) signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter [Multi-Faktor-Authentifizierung](#) im AWS IAM Identity Center - Benutzerhandbuch und [Verwenden der Multi-Faktor-Authentifizierung \(MFA\) in AWS](#) im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie ein AWS-Konto erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter [Was ist IAM Identity Center?](#) im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Eine [IAM-Gruppe](#) ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter [Erstellen eines IAM-Benutzers \(anstatt einer Rolle\)](#) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen [wechseln](#). Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter [Verwenden von IAM-Rollen](#) im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- **Verbundbenutzerzugriff:** Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter [Erstellen von Rollen für externe](#)

[Identitätsanbieter](#) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze](#) im AWS IAM Identity Center -Benutzerhandbuch.

- Temporäre IAM-Benutzerberechtigungen: Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien](#) im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
- Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).
- Servicerolle: Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem

Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Anwendungen, die auf Amazon EC2 ausgeführt werden — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter [Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden](#) im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter [Erstellen einer IAM-Rolle \(anstatt eines Benutzers\)](#) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter [Auswahl zwischen verwalteten und eingebundenen Richtlinien](#) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen zu ACLs finden Sie unter [Zugriffssteuerungsliste \(ACL\) – Übersicht](#) (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- **Berechtigungsgrenzen:** Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im IAM-Benutzerhandbuch.
- **Service Control Policies (SCPs)** — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten, die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organisationen und SCPs finden Sie unter [Funktionsweise von SCPs](#) im AWS Organizations -Benutzerhandbuch.
- **Sitzungsrichtlinien:** Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und

der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

Wie AWS Shield funktioniert mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Shield zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für Shield verfügbar sind.

IAM-Funktionen, die Sie mit verwenden können AWS Shield

IAM-Feature	Shield-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (servicespezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Ja

IAM-Feature	Shield-Unterstützung
Service-verknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie Shield und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im [IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren](#).

Identitätsbasierte Richtlinien für Shield

Unterstützt Richtlinien auf Identitätsbasis.	Ja
--	----

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Shield-Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Shield](#)

Ressourcenbasierte Richtlinien innerhalb von Shield

Unterstützt ressourcenbasierte Richtlinien	Nein
--	------

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern.

Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter [Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden](#) im IAM-Benutzerhandbuch.

Politische Maßnahmen für Shield

Unterstützt Richtlinienaktionen

Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der Shield-Aktionen finden Sie unter [Aktionen definiert von AWS Shield](#) in der Service Authorization Reference.

Richtlinienaktionen in Shield verwenden vor der Aktion das folgende Präfix:

```
shield
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [  
  "shield:action1",  
  "shield:action2"  
]
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Um beispielsweise alle Aktionen in Shield anzugeben, die mit `beginnenList`, schließen Sie die folgende Aktion ein:

```
"Action": "shield:List*"
```

Beispiele für identitätsbasierte Shield-Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Shield](#)

Politische Ressourcen für Shield

Unterstützt Richtlinienressourcen	Ja
-----------------------------------	----

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein `Resource` oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen [Amazon-Ressourcennamen \(ARN\)](#) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"

```

Eine Liste der Shield-Ressourcentypen und ihrer ARNs finden Sie unter [Resources defined by AWS Shield](#) in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter [Von AWS Shield definierte Aktionen](#). Um den Zugriff auf eine Teilmenge der Shield-Ressourcen zu erlauben oder zu verweigern, nehmen Sie den ARN der Ressource in das `resource` Element Ihrer Richtlinie auf.

Bei AWS Shield den Ressourcen handelt es sich um Schutzmaßnahmen und Angriffe. Diesen Ressourcen sind einzigartige Amazon-Ressourcennamen (ARN) zugeordnet, siehe nachfolgende Tabelle.

Name in der Konsole AWS Shield	Name im AWS Shield SDK/ CLI	ARN-Format
Ereignis oder Angriff	AttackDetail	arn:aws:shield:: <i>account</i> :attack/ <i>ID</i>
Schutz	Protection	arn:aws:shield:: <i>account</i> :protection/ <i>ID</i>

Um den Zugriff auf eine Teilmenge der Shield-Ressourcen zu erlauben oder zu verweigern, nehmen Sie den ARN der Ressource in das `resource` Element Ihrer Richtlinie auf. Die ARNs für Shield haben das folgende Format:

```
arn:partition:shield::account:resource/ID

```

Ersetzen Sie Variablen für *Konto*, *Ressource* und *ID* durch gültige Werte. Gültige Werte können beispielsweise folgende sein:

- *Konto*: Die ID Ihres AWS-Konto. Sie müssen einen Wert angeben.
- *resource*: Der Typ der Shield-Ressource, entweder `attack` oder `protection`.
- *ID*: Die ID der Shield-Ressource oder ein Platzhalter (*), um alle Ressourcen des angegebenen Typs anzugeben, die mit der angegebenen AWS-Konto Ressource verknüpft sind.

Der folgende ARN gibt zum Beispiel alle Schutzmaßnahmen für das Konto 111122223333 an:

```
arn:aws:shield::111122223333:protection/*
```

Die ARNs der Shield-Ressourcen haben das folgende Format:

```
arn:partition:shield:region:account-id:scope/resource-type/resource-name/resource-id
```

Allgemeine Informationen zu ARN-Spezifikationen finden Sie unter [Amazon Resource Names \(ARNs\)](#) in der Allgemeine Amazon Web Services-Referenz.

Im Folgenden sind die spezifischen Anforderungen für die ARNs von wafv2 Ressourcen aufgeführt:

- **Region:** Für Shield-Ressourcen, die Sie zum Schutz von CloudFront Amazon-Distributionen verwenden, setzen Sie diesen Wert auf `us-east-1`. Andernfalls legen Sie hier die Region fest, die Sie mit Ihren geschützten regionalen Ressourcen verwenden.
- **Umfang:** Legen Sie den Geltungsbereich auf `global` für die Verwendung mit einer CloudFront Amazon-Distribution oder `regional` für die Verwendung mit einer der regionalen Ressourcen fest, die dies AWS WAF unterstützen. Bei den regionalen Ressourcen handelt es sich um eine Amazon API Gateway Gateway-REST-API, einen Application Load Balancer, eine AWS AppSync GraphQL-API, einen Amazon Cognito Cognito-Benutzerpool, einen AWS App Runner Service und eine AWS Verified Access-Instance.
- **Ressourcentyp:** Geben Sie einen der folgenden Werte an: `attack` für Ereignisse oder Angriffe, für Schutzmaßnahmen. `protection`
- **Ressourcename:** Geben Sie den Namen an, den Sie der Shield-Ressource gegeben haben, oder geben Sie einen Platzhalter (*) an, um alle Ressourcen anzugeben, die die anderen Spezifikationen im ARN erfüllen. Sie müssen entweder den Ressourcennamen und die Ressourcen-ID oder einen Platzhalter für beide angeben.
- **resource-id:** Geben Sie die ID der Shield-Ressource an, oder geben Sie einen Platzhalter (*) an, um alle Ressourcen anzugeben, die die anderen Spezifikationen im ARN erfüllen. Sie müssen entweder den Ressourcennamen und die Ressourcen-ID oder für beide einen Platzhalter angeben.

Der folgende ARN gibt zum Beispiel alle Web-ACLs mit regionalem Geltungsbereich für das Konto 111122223333 in Region `us-west-1` an:

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

Der folgende ARN gibt die Regelgruppe an, die MyIPManagementRuleGroup mit dem globalen Geltungsbereich für das Konto 111122223333 in Region benannt ist us-east-1:

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

Beispiele für identitätsbasierte Shield-Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Shield](#)

Schlüssel zu den Policy-Bedingungen für Shield

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Ja
---	----

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition block`) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die [Bedingungsoperatoren](#) verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen OR Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter [IAM-Richtlinienelemente: Variablen und Tags](#) im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [Kontextschlüssel für AWS globale Bedingungen](#) im IAM-Benutzerhandbuch.

Eine Liste der Shield-Bedingungsschlüssel finden Sie unter [Bedingungsschlüssel für AWS Shield](#) in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter [Aktionen definiert von AWS Shield](#).

Beispiele für identitätsbasierte Shield-Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Shield](#)

ACLs in Shield

Unterstützt ACLs	Nein
------------------	------

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit Shield

Unterstützt ABAC (Tags in Richtlinien)	Teilweise
--	-----------

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement einer [Richtlinie Tag-Informationen](#) an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter [Was ist ABAC?](#) im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe [Attributbasierte Zugriffskontrolle \(ABAC\)](#) verwenden im IAM-Benutzerhandbuch.

Temporäre Anmeldeinformationen mit Shield verwenden

Unterstützt temporäre Anmeldeinformationen	Ja
--	----

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services [funktionieren AWS-Services](#) , [finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM](#).

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter [Wechseln zu einer Rolle \(Konsole\)](#) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter [Temporäre Sicherheitsanmeldeinformationen in IAM](#).

Zugriffssitzungen für Shield weiterleiten

Unterstützt Forward Access Sessions (FAS)	Ja
---	----

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren

Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

Servicerollen für Shield

Unterstützt Servicerollen	Ja
---------------------------	----

Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.

Warning

Durch das Ändern der Berechtigungen für eine Servicerolle kann die Shield-Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, wenn Shield Sie dazu anleitet.

Servicebezogene Rollen für Shield

Unterstützt serviceverknüpfte Rollen	Ja
--------------------------------------	----

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer [Service-Verknüpfung](#) ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstverknüpften Shield-Rollen finden Sie unter [Verwenden von serviceverknüpften Rollen für Shield Advanced](#).

Beispiele für identitätsbasierte Richtlinien für AWS Shield

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Shield-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien

erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Einzelheiten zu den von Shield definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden der Ressourcentypen, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Shield](#) in der Service Authorization Reference.

Themen

- [Bewährte Methoden für Richtlinien](#)
- [Verwenden der Shield-Konsole](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)
- [Gewähren Sie Lesezugriff auf Ihre Shield Advanced-Schutzmaßnahmen](#)
- [Gewähren Sie nur Lesezugriff auf Shield, und CloudFront CloudWatch](#)
- [Vollzugriff auf Shield gewähren CloudFront, und CloudWatch](#)

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Shield-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter [AWS -verwaltete Richtlinien](#) oder [AWS -verwaltete Richtlinien für Auftrags-Funktionen](#) im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten: Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer

Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter [Richtlinien und Berechtigungen in IAM](#) im IAM-Benutzerhandbuch.

- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs: Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: Bedingung](#) im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten: IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter [Richtliniengültigkeit zum IAM Access Analyzer](#) im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter [Konfigurieren eines MFA-geschützten API-Zugriffs](#) im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Bewährte Methoden für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

Verwenden der Shield-Konsole

Um auf die AWS Shield Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Shield-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Benutzer, die auf die AWS Konsole zugreifen und sie verwenden können, können auch auf die AWS Shield Konsole zugreifen. Es sind keine zusätzlichen Berechtigungen erforderlich.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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": "*"
    }
  ]
}
```

```

    }
  ]
}

```

Gewähren Sie Lesezugriff auf Ihre Shield Advanced-Schutzmaßnahmen

AWS Shield ermöglicht den kontoübergreifenden Zugriff auf Ressourcen, ermöglicht Ihnen jedoch nicht, kontenübergreifende Schutzmaßnahmen für Ressourcen einzurichten. Sie können Schutz für Ressourcen nur aus dem Konto erstellen, das der Besitzer dieser Ressourcen ist.

Es folgt ein Beispiel für eine Richtlinie, die Berechtigungen für die `shield:ListProtections`-Aktionen für alle Ressourcen erteilt. Shield unterstützt nicht die Identifizierung bestimmter Ressourcen mithilfe der Ressourcen-ARNs (auch als Berechtigungen auf Ressourcenebene bezeichnet) für einige API-Aktionen, daher geben Sie ein Platzhalterzeichen (*) an. Dies ermöglicht nur den Zugriff auf die Ressourcen, die Sie durch die Aktion abrufen können. `ListProtections`

```

{
  "Version": "2016-06-02",
  "Statement": [
    {
      "Sid": "ListProtections",
      "Effect": "Allow",
      "Action": [
        "shield:ListProtections"
      ],
      "Resource": "*"
    }
  ]
}

```

Gewähren Sie nur Lesezugriff auf Shield,, und CloudFront CloudWatch

Die folgende Richtlinie gewährt Benutzern nur Lesezugriff auf Shield und zugehörige Ressourcen, einschließlich CloudFront Amazon-Ressourcen und CloudWatch Amazon-Metriken. Es ist nützlich für Benutzer, die die Erlaubnis benötigen, die Einstellungen in Shield Protections and Attacks einzusehen und Metriken zu überwachen. CloudWatch Diese Benutzer können keine Shield-Ressourcen erstellen, aktualisieren oder löschen.

```

{
  "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": "*"
    }
  ]
}

```

Vollzugriff auf Shield gewähren CloudFront, und CloudWatch

Mit der folgenden Richtlinie können Benutzer alle Shield-Operationen und alle Operationen auf CloudFront Webverteilungen ausführen sowie Metriken und eine Stichprobe von Anfragen in CloudWatch überwachen. Es ist nützlich für Benutzer, die Shield-Administratoren sind.

```

{
  "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": "*"
    }
  ]
}

```

Es wird dringend empfohlen, dass Sie die Multi-Factor Authentication (MFA, Multifaktor-Authentifizierung) für Benutzer mit Administrator-Berechtigungen konfigurieren. Weitere

Informationen finden Sie unter [Using Multi-Factor Authentication \(MFA\) -Geräte mit AWS](#) im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinien für AWS Shield

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie für alle AWS Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie [kundenverwaltete Richtlinien](#) definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter [Von AWS verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSShieldDRTAccessPolicy

AWS Shield verwendet diese verwaltete Richtlinie, wenn Sie dem Shield Response Team (SRT) die Erlaubnis erteilen, in Ihrem Namen zu handeln. Diese Richtlinie gewährt dem SRT eingeschränkten Zugriff auf Ihr AWS Konto, um Sie bei der Abwehr von DDoS-Angriffen bei Ereignissen mit hohem Schweregrad zu unterstützen. Diese Richtlinie ermöglicht es der SRT, Ihre AWS WAF Regeln und Shield Advanced-Schutzmaßnahmen zu verwalten und auf Ihre AWS WAF Protokolle zuzugreifen.

Informationen darüber, wie Sie der SRT die Erlaubnis erteilen, in Ihrem Namen tätig zu werden, finden Sie unter [Konfiguration des Zugriffs für das Shield Response Team \(SRT\)](#)

Einzelheiten zu dieser Richtlinie finden Sie unter [AWSShieldDRTAccessPolicy](#) in der IAM-Konsole.

AWS verwaltete Richtlinie: AWSShieldServiceRolePolicy

Shield Advanced verwendet diese verwaltete Richtlinie, wenn Sie die automatische DDoS-Abwehr auf Anwendungsebene aktivieren, um die Berechtigungen festzulegen, die für die Verwaltung der

Ressourcen für Ihr Konto erforderlich sind. Diese Richtlinie ermöglicht Shield Advanced, AWS WAF Regeln und Regelgruppen in den Web-ACLs zu erstellen und anzuwenden, die Sie Ihren geschützten Ressourcen zugeordnet haben, um automatisch auf DDoS-Angriffe zu reagieren.

Sie können keine Verbindungen `AWSShieldServiceRolePolicy` zu Ihren IAM-Entitäten herstellen. Shield fügt diese Richtlinie der dienstbezogenen Rolle hinzu `AWSServiceRoleForAWSShield`, damit Shield Aktionen in Ihrem Namen durchführen kann.

Shield Advanced ermöglicht die Verwendung dieser Richtlinie, wenn Sie die automatische DDoS-Abwehr auf Anwendungsebene aktivieren. Weitere Informationen zur Verwendung dieser Richtlinie finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#)

Informationen zur dienstbezogenen Rolle `AWSServiceRoleForAWSShield`, die diese Richtlinie verwendet, finden Sie unter [Verwenden von serviceverknüpften Rollen für Shield Advanced](#)

Einzelheiten zu dieser Richtlinie finden Sie unter [AWSShieldServiceRolePolicy](#) in der IAM-Konsole.

Shield-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Shield an, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Für automatische Benachrichtigungen über Änderungen an dieser Seite abonnieren Sie den RSS-Feed auf der Shield-Dokumentenverlaufsseite unter [Dokumentverlauf](#).

Richtlinie	Beschreibung der Änderung	Datum
<p><code>AWSShieldServiceRolePolicy</code></p> <p>Diese Richtlinie ermöglicht Shield den Zugriff auf und die Verwaltung von AWS Ressourcen, um in Ihrem Namen automatisch auf DDoS-Angriffe auf Anwendungsebene zu reagieren.</p>	<p>Diese Richtlinie wurde hinzugefügt, um Shield Advanced die Berechtigungen zu gewähren, die für die automatische DDoS-Abwehr auf Anwendungsebene erforderlich sind. Informationen zu dieser Funktion finden Sie unter Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene</p>	1. Dezember 2021

Richtlinie	Beschreibung der Änderung	Datum
<p>Einzelheiten in der IAM-Konsole: AWSShieldServiceRolePolicy</p> <p>Die serviceverknüpfte Rolle AWSServiceRoleForAWSShield verwendet diese Richtlinie. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Shield Advanced.</p>		
Shield hat begonnen, Änderungen zu verfolgen	Shield begann, Änderungen für seine AWS verwalteten Richtlinien zu verfolgen.	3. März 2021

Problembehandlung bei AWS Shield Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Shield und IAM auftreten können.

Themen

- [Ich bin nicht berechtigt, eine Aktion in Shield durchzuführen](#)
- [Ich bin nicht berechtigt, iam auszuführen: PassRole](#)
- [Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Shield-Ressourcen ermöglichen](#)

Ich bin nicht berechtigt, eine Aktion in Shield durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven `my-example-widget`-Ressource anzuzeigen, jedoch nicht über `shield:GetWidget`-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
shield:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `shield:GetWidget`-Aktion auf die `my-example-widget`-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Shield übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Shield auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Shield-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffssteuerungslisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Shield diese Funktionen unterstützt, finden Sie unter [Wie AWS Shield funktioniert mit IAM](#).
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter [Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto, den Sie besitzen](#).
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter [Gewähren von Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien](#) im IAM-Benutzerhandbuch.

Verwenden von serviceverknüpften Rollen für Shield Advanced

AWS Shield Advanced [verwendet AWS Identity and Access Management \(IAM\) serviceverknüpfte Rollen](#). Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Shield Advanced verknüpft ist. Dienstbezogene Rollen sind von Shield Advanced vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle erleichtert die Einrichtung von Shield Advanced, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Shield Advanced definiert die Berechtigungen seiner dienstbezogenen Rollen, und sofern nicht anders definiert, kann nur Shield Advanced seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und

Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre Shield Advanced-Ressourcen, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceverknüpften Rollen unterstützen, finden Sie unter [AWS -Services, die mit IAM funktionieren](#). Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Dienstbezogene Rollenberechtigungen für Shield Advanced

Shield Advanced verwendet die mit dem Dienst verknüpfte Rolle namens `AWSServiceRoleForAWSShield`. Diese Rolle ermöglicht Shield Advanced den Zugriff auf und die Verwaltung von AWS Ressourcen, um in Ihrem Namen automatisch auf DDoS-Angriffe auf Anwendungsebene zu reagieren. Weitere Informationen zu dieser Funktion finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#).

Die `AWSServiceRoleForAWSShield` dienstverknüpfte Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `shield.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie `AWSShieldServiceRolePolicy` ermöglicht es Shield Advanced, die folgenden Aktionen für alle AWS Ressourcen durchzuführen:

- `wafv2:GetWebACL`
- `wafv2:UpdateWebACL`
- `wafv2:GetWebACLForResource`
- `wafv2:ListResourcesForWebACL`
- `cloudfront:ListDistributions`
- `cloudfront:GetDistribution`

Wenn Aktionen für alle AWS Ressourcen zulässig sind, wird dies in der Richtlinie als angegeben `"Resource": "*"` . Dies bedeutet lediglich, dass die dienstbezogene Rolle jede

angegebene Aktion für alle AWS Ressourcen ausführen kann, die von der Aktion unterstützt werden. Die Aktion `wafv2:GetWebACL` wird beispielsweise nur für `wafv2` Web-ACL-Ressourcen unterstützt.

Shield Advanced führt nur API-Aufrufe auf Ressourcenebene für geschützte Ressourcen durch, für die Sie die Schutzfunktion auf Anwendungsebene aktiviert haben, und für Web-ACLs, die diesen geschützten Ressourcen zugeordnet sind.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [serviceverknüpfte Rollenberechtigungen](#) im IAM-Benutzerhandbuch.

Eine serviceverknüpfte Rolle für Shield Advanced erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie die automatische DDoS-Abwehr auf Anwendungsebene für eine Ressource in der AWS Management Console, der oder der AWS API aktivieren AWS CLI, erstellt Shield Advanced die dienstbezogene Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie die automatische DDoS-Abwehr auf Anwendungsebene für eine Ressource aktivieren, erstellt Shield Advanced die dienstbezogene Rolle erneut für Sie.

Bearbeiten einer serviceverknüpften Rolle für Shield Advanced

Shield Advanced erlaubt es Ihnen nicht, die `AWSServiceRoleForAWSShield` serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Shield Advanced

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpften Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Note

Wenn Shield Advanced die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um die Shield Advanced-Ressourcen zu löschen, die von `AWSServiceRoleForAWSShield`

Deaktivieren Sie für all Ihre Ressourcen, für die der DDoS-Schutz auf Anwendungsebene konfiguriert ist, die automatische DDoS-Abwehr auf Anwendungsebene. Anweisungen für die Konsole finden Sie unter [Konfigurieren Sie den DDoS-Schutz auf Anwendungsebene](#)

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die `AWSServiceRoleForAWSShield` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Leitfaden.

Unterstützte Regionen für Service-verknüpfte Shield Advanced-Rollen

Shield Advanced unterstützt die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter [Shield Advanced-Endpunkte und Kontingente](#).

Protokollierung und Überwachung in Shield

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Shield und Ihren AWS Lösungen. Sie sollten Überwachungsdaten aus allen Teilen Ihrer AWS Lösung sammeln, damit Sie einen etwaigen Ausfall an mehreren Stellen leichter debuggen können. AWS bietet verschiedene Tools zur Überwachung Ihrer Shield-Ressourcen und zur Reaktion auf potenzielle Ereignisse:

CloudWatch Amazon-Alarme

Mithilfe von CloudWatch Alarmen beobachten Sie eine einzelne Metrik über einen von Ihnen festgelegten Zeitraum. Wenn die Metrik einen bestimmten Schwellenwert überschreitet, CloudWatch sendet eine Benachrichtigung an ein Amazon SNS SNS-Thema oder eine AWS Auto Scaling Richtlinie. Weitere Informationen finden Sie unter [Überwachung mit Amazon CloudWatch](#).

AWS CloudTrail Logs

CloudTrail bietet eine Aufzeichnung der Aktionen, die von einem Benutzer, einer Rolle oder einem AWS Dienst in Shield ausgeführt wurden. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Shield gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln. Weitere Informationen finden Sie unter [Protokollierung von AWS CloudTrail-API-Aufrufen mit](#).

Konformitätsvalidierung für Shield

Informationen darüber, ob AWS-Service ein [AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter](#) . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter [AWS Compliance-Programme AWS](#) .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter [Berichte herunterladen unter](#) .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- [Schnellstartanleitungen zu Sicherheit und Compliance](#) — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

Note

AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der [Referenz für HIPAA-berechtigte Services](#).

- [AWS Compliance-Ressourcen](#) — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- [AWS Leitfäden zur Einhaltung von Vorschriften für Kunden](#) — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- [Evaluierung von Ressourcen anhand von Regeln](#) im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.

- [AWS Security Hub](#)— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der [Security-Hub-Steuerungsreferenz](#).
- [AWS Audit Manager](#)— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz in Shield

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter [AWS Globale](#) Infrastruktur.

Sicherheit der Infrastruktur in AWS Shield

Als verwalteter Dienst AWS Shield ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter [AWS Cloud-Sicherheit](#). Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Shield zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit [AWS Security Token Service](#) (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

AWS Shield Advanced Kontingente

AWS Shield Advanced hat Standardkontingente für die Anzahl der Entitäten pro Region. Sie können [eine Erhöhung dieser Kontingente beantragen](#).

Ressource	Standardkontingent
Maximale Anzahl geschützter Ressourcen für jeden Ressourcentyp, der Schutz AWS Shield Advanced bietet, pro Konto.	1.000
Maximale Anzahl von Schutzgruppen pro Konto.	100
Maximale Anzahl einzelner geschützter Ressourcen, die Sie speziell in eine Schutzgruppe aufnehmen können. In der API bezieht sich dies auf <code>Members</code> die, die Sie bei der Einstellung der Schutzgruppe <code>Pattern</code> angeben <code>ARBITRARY</code> . In der Konsole gilt dies für die Ressourcen, die Sie für die Schutzgruppe Wählen Sie aus geschützten Ressourcen auswählen auswählen.	1.000

AWS Firewall Manager

AWS Firewall Manager vereinfacht Ihre Verwaltungs- und Wartungsaufgaben für mehrere Konten und Ressourcen und bietet eine Vielzahl von Schutzmaßnahmen AWS WAF AWS Shield Advanced, darunter Amazon VPC-Sicherheitsgruppen und Amazon Route 53 Resolver DNS Firewall. AWS Network Firewall Mit Firewall Manager richten Sie Ihre Schutzmaßnahmen nur einmal ein und der Service wendet sie automatisch auf Ihre Konten und Ressourcen an, auch wenn Sie neue Konten und Ressourcen hinzufügen.

Firewall Manager bietet folgende Vorteile:

- Schützt Ressourcen kontoübergreifend.
- Hilft dabei, alle Ressourcen eines bestimmten Typs zu schützen, z. B. alle CloudFront Amazon-Distributionen
- Schützt alle Ressourcen mit bestimmten Tags.
- Wendet den Schutz automatisch auf Ressourcen an, die zu Ihrem Konto hinzugefügt werden.
- Ermöglicht es Ihnen, alle Mitgliedskonten einer AWS Organizations Organisation zu abonnieren AWS Shield Advanced, und abonniert automatisch neue Konten, die der Organisation beitreten
- Ermöglicht das Anwenden von Sicherheitsgruppenregeln auf alle Mitgliedskonten oder bestimmte Teilmengen von Konten in einer AWS Organizations -Organisation und wendet die Regeln automatisch auf neue Konten innerhalb des Bereichs an, die der Organisation beitreten.
- Ermöglicht es Ihnen, Ihre eigenen Regeln zu verwenden oder verwaltete Regeln von zu erwerben AWS Marketplace

Firewall Manager ist besonders nützlich, wenn Sie Ihr gesamtes Unternehmen schützen möchten und nicht nur eine kleine Anzahl bestimmter Konten und Ressourcen, oder wenn Sie häufig neue Ressourcen hinzufügen, die Sie schützen möchten. Firewall Manager bietet auch eine zentrale Überwachung von DDoS-Angriffen in Ihrem gesamten Unternehmen.

Themen

- [AWS Firewall Manager Preisgestaltung](#)
- [AWS Firewall Manager Voraussetzungen](#)
- [Zusammenarbeit mit AWS Firewall Manager Administratoren](#)
- [Erste Schritte mit AWS Firewall Manager Richtlinien](#)

- [Mit AWS Firewall Manager Richtlinien arbeiten](#)
- [Arbeiten mit Ressourcensätzen in Firewall Manager](#)
- [Compliance-Informationen für eine AWS Firewall Manager Richtlinie anzeigen](#)
- [AWS Firewall Manager Befunde](#)
- [Sicherheit in AWS Firewall Manager](#)
- [AWS Firewall Manager Kontingente](#)

AWS Firewall Manager Preisgestaltung

Gebühren, die AWS Firewall Manager anfallen, beziehen sich auf die zugrunde liegenden Dienste wie AWS WAF und AWS Config. Weitere Informationen finden Sie unter [AWS Firewall Manager - Preise](#).

AWS Firewall Manager Voraussetzungen

In diesem Thema erfahren Sie, wie Sie sich auf die Verwaltung AWS Firewall Manager vorbereiten. Sie verwenden ein Firewall Manager Manager-Administratorkonto, um alle Firewall Manager Manager-Sicherheitsrichtlinien für Ihr Unternehmen in zu verwalten AWS Organizations. Sofern nicht anders angegeben, führen Sie die erforderlichen Schritte mit dem Konto aus, das Sie als Firewall Manager Manager-Administrator verwenden werden.

Bevor Sie Firewall Manager zum ersten Mal verwenden, führen Sie die folgenden Schritte nacheinander aus.

Themen

- [Schritt 1: Beitreten und konfigurieren AWS Organizations](#)
- [Schritt 2: Erstellen Sie ein AWS Firewall Manager Standard-Administratorkonto](#)
- [Schritt 3: Aktivieren AWS Config](#)
- [Schritt 4: Abonnieren Sie Richtlinien für Drittanbieter im AWS Marketplace und konfigurieren Sie die Drittanbieter-Einstellungen](#)
- [Schritt 5: Aktivieren Sie für Network Firewall- und DNS-Firewall-Richtlinien die gemeinsame Nutzung von Ressourcen](#)
- [Schritt 6: Zur Verwendung AWS Firewall Manager in Regionen, die standardmäßig deaktiviert sind](#)

Schritt 1: Beitreten und konfigurieren AWS Organizations

Um Firewall Manager verwenden zu können, muss Ihr Konto Mitglied der Organisation in dem AWS Organizations Dienst sein, für den Sie Ihre Firewall Manager Manager-Richtlinien verwenden möchten.

Note

Informationen zu Organizations finden Sie im [AWS Organizations Benutzerhandbuch](#).

So richten Sie die erforderliche AWS Organizations Mitgliedschaft und Konfiguration ein

1. Wählen Sie unter Organizations ein Konto aus, das als Firewall Manager Manager-Administrator für die Organisation verwendet werden soll.
2. Wenn das von Ihnen gewählte Konto noch kein Mitglied der Organisation ist, lassen Sie es beitreten. Folgen Sie den Anweisungen unter [Einen AWS-Konto einladen, Ihrer Organisation beizutreten](#).
3. AWS Organizations verfügt über zwei verfügbare Funktionen: Funktionen zur konsolidierten Abrechnung und alle Funktionen. Um Firewall Manager verwenden zu können, muss Ihr Unternehmen für alle Funktionen aktiviert sein. Wenn Ihre Organisation nur für die konsolidierte Fakturierung konfiguriert ist, folgen Sie den Anweisungen unter [Alle Funktionen in Ihrer Organisation aktivieren](#).

Schritt 2: Erstellen Sie ein AWS Firewall Manager Standard-Administratorkonto

Bei diesem Verfahren werden das Konto und die Organisation verwendet, die Sie im vorherigen Schritt ausgewählt und konfiguriert haben.

Nur das Verwaltungskonto der Organisation kann Firewall Manager Manager-Standardadministratorkonten erstellen. Das erste Administratorkonto, das Sie erstellen, ist das Standard-Administratorkonto. Das Standard-Administratorkonto kann Firewalls von Drittanbietern verwalten und hat vollen administrativen Umfang. Wenn Sie das Standard-Administratorkonto einrichten, legt Firewall Manager es automatisch als AWS Organizations delegierten Administrator für Firewall Manager fest. Dadurch kann Firewall Manager auf Informationen über die

Organisationseinheiten (OUs) in der Organisation zugreifen. Sie können Organisationseinheiten verwenden, um den Geltungsbereich Ihrer Firewall Manager Manager-Richtlinien festzulegen. Weitere Informationen zur Festlegung des Geltungsbereichs von Richtlinien finden Sie in den Anleitungen für die einzelnen Richtlinientypen unter [Eine AWS Firewall Manager Richtlinie erstellen](#). Weitere Informationen zu Organizations und Verwaltungskonten finden Sie unter [AWS Konten in Ihrer Organisation verwalten](#).

Erforderliche Einstellungen für das Verwaltungskonto der Organisation

Das Verwaltungskonto der Organisation muss über die folgenden Einstellungen verfügen, um die Organisation in Firewall Manager einzubinden und einen Standardadministrator zu erstellen:

- Es muss ein Mitglied der Organisation sein, AWS Organizations in der Sie Ihre Firewall Manager Manager-Richtlinien anwenden möchten.

Um das Standard-Administratorkonto einzurichten

1. Melden Sie sich AWS Management Console mit einem vorhandenen AWS Organizations Verwaltungskonto beim Firewall Manager an.
2. Öffnen Sie die Firewall Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>.
3. Wählen Sie im Navigationsbereich Settings (Einstellungen).
4. Geben Sie die AWS Konto-ID des Kontos ein, das Sie als Firewall Manager Manager-Administrator verwenden möchten.

Note

Der Standardadministrator hat den vollen administrativen Bereich. Vollständiger administrativer Geltungsbereich bedeutet, dass dieses Konto Richtlinien auf alle Konten und Organisationseinheiten (OUs) innerhalb der Organisation anwenden, Aktionen in allen Regionen ergreifen und alle Firewall Manager Manager-Richtlinientypen verwalten kann.

5. Wählen Sie Administratorkonto erstellen, um das Konto zu erstellen.

Weitere Informationen zur Verwaltung des Firewall Manager Manager-Administratorkontos finden Sie unter [Zusammenarbeit mit AWS Firewall Manager Administratoren](#).

Schritt 3: Aktivieren AWS Config

Um den Firewall Manager verwenden zu können, müssen Sie ihn aktivieren AWS Config.

Note

Für Ihre AWS Config Einstellungen fallen je nach AWS Config Preisgestaltung Gebühren an. Weitere Informationen finden Sie unter [Erste Schritte mit AWS Config](#).

Note

Damit Firewall Manager die Einhaltung der Richtlinien überwachen kann, AWS Config müssen die Konfigurationsänderungen für geschützte Ressourcen kontinuierlich aufgezeichnet werden. In Ihrer AWS Config Konfiguration muss die Aufzeichnungsfrequenz auf kontinuierlich eingestellt sein, was die Standardeinstellung ist.

Zur Aktivierung AWS Config für Firewall Manager

1. Aktivieren Sie AWS Config diese Option für jedes Ihrer AWS Organizations Mitgliedskonten, einschließlich des Firewall Manager Manager-Administratorkontos. Weitere Informationen finden Sie unter [Erste Schritte mit AWS Config](#).
2. Aktivieren Sie AWS-Region diese Option AWS Config für jede Ressource, die die Ressourcen enthält, die Sie schützen möchten. Sie können die AWS Config Option manuell aktivieren oder die AWS CloudFormation Vorlage „Aktivieren AWS Config“ unter [AWS CloudFormation StackSets Beispielvorlagen](#) verwenden.

Wenn Sie die Aktivierung nicht AWS Config für alle Ressourcen durchführen möchten, müssen Sie je nach Art der verwendeten Firewall Manager Manager-Richtlinien Folgendes aktivieren:

- WAF-Richtlinie — Aktivieren Sie Config für die Ressourcentypen CloudFront Distribution, Application Load Balancer (wählen Sie ElasticLoadBalancingV2 aus der Liste), API Gateway, WAF WebACL, WAF Regional WebACL und WAFv2 WebACL. Um eine CloudFront Distribution zu aktivieren AWS Config oder zu schützen, müssen Sie sich in der Region USA Ost (Nord-Virginia) befinden. In anderen Regionen ist diese CloudFront Option nicht verfügbar.

- **Shield-Richtlinie** — Aktivieren Sie Config für die Ressourcentypen Shield Protection, ShieldRegional Protection, Application Load Balancer, EC2 EIP, WAF WebACL, WAF Regional WebACL und WAFv2 WebACL.
- **Sicherheitsgruppenrichtlinie** — Aktivieren Sie Config für die Ressourcentypen EC2 SecurityGroup, EC2 Instance und EC2. NetworkInterface
- **Netzwerk-Firewall-Richtlinie** — Aktivieren Sie Config für die Ressourcentypen NetworkFirewall FirewallPolicy EC2 VPC, EC2 InternetGateway, EC2 und EC2 Subnet RouteTable. NetworkFirewall RuleGroup
- **DNS-Firewall-Richtlinie** — Aktivieren Sie Config für den Ressourcentyp EC2 VPC.
- **Firewall-Richtlinie von Drittanbietern** — Aktivieren Sie Config für die Ressourcentypen Amazon EC2 VPC, Amazon EC2, Amazon EC2 InternetGateway, Amazon EC2 RouteTable Subnet und Amazon EC2 VPCEndpoint.

Note

Wenn Sie Ihren AWS Config Rekorder für die Verwendung einer benutzerdefinierten IAM-Rolle konfigurieren, müssen Sie sicherstellen, dass die IAM-Richtlinie über die richtigen Berechtigungen verfügt, um die erforderlichen Ressourcentypen der Firewall Manager Manager-Richtlinie aufzuzeichnen. Ohne die entsprechenden Berechtigungen werden die erforderlichen Ressourcen möglicherweise nicht aufgezeichnet, sodass Firewall Manager Ihre Ressourcen nicht ordnungsgemäß schützen kann. Firewall Manager hat keinen Einblick in diese Fehlkonfigurationen von Berechtigungen. Informationen zur Verwendung von IAM mit AWS Config finden Sie unter [IAM](#) for. AWS Config

Schritt 4: Abonnieren Sie Richtlinien für Drittanbieter im AWS Marketplace und konfigurieren Sie die Drittanbieter-Einstellungen

Erfüllen Sie die folgenden Voraussetzungen, um mit den Firewall-Richtlinien von Drittanbietern von Firewall Manager zu beginnen.

Voraussetzungen für die Fortigate Cloud Native Firewall (CNF) as a Service-Richtlinie

Um Fortigate CNF für Firewall Manager zu verwenden

1. Abonnieren Sie den [Fortigate Cloud Native Firewall \(CNF\) as a Service Service](#) im Marketplace. AWS
2. Registrieren Sie zunächst einen Mandanten auf dem Fortigate CNF-Produktportal. Fügen Sie dann Ihr Firewall Manager Administratorkonto unter Ihrem Mandanten im Fortigate CNF-Produktportal hinzu. Weitere Informationen finden Sie in der [Fortigate CNF-Dokumentation](#).

Informationen zur Arbeit mit Fortigate CNF-Richtlinien finden Sie unter. [Richtlinien für die Fortigate Cloud Native Firewall \(CNF\) als Service](#)

Voraussetzungen für die Cloud-Firewall-Richtlinie der nächsten Generation von Palo Alto Networks

So verwenden Sie Palo Alto Networks Cloud NGFW für Firewall Manager

1. Abonnieren Sie den [Pay-As-You-Go-Dienst Palo Alto Networks Cloud Next Generation Firewall](#) auf dem Marketplace. AWS
2. Führen Sie die im Abschnitt [Deploy Palo Alto Networks Cloud NGFW für Deploy Palo Alto Networks Cloud NGFW aufgeführten Schritte zur Bereitstellung von Palo Alto Networks Cloud NGFW anhand des AWS Firewall Manager Themas im Leitfaden Palo Alto Networks Cloud Next AWS Generation Firewall for Deployment](#) durch. AWS

Informationen zur Arbeit mit den NGFW-Richtlinien der Palo Alto Networks Cloud finden Sie unter. [NGFW-Richtlinien für die Cloud von Palo Alto Networks](#)

Schritt 5: Aktivieren Sie für Network Firewall- und DNS-Firewall-Richtlinien die gemeinsame Nutzung von Ressourcen

Um die Netzwerkfirewall- und DNS-Firewall-Richtlinien von Firewall Manager zu verwalten, müssen Sie die gemeinsame Nutzung mit AWS Organizations in aktivieren AWS Resource Access Manager. Auf diese Weise kann Firewall Manager Schutzmaßnahmen für Ihre Konten bereitstellen, wenn Sie diese Richtlinientypen erstellen.

Um das Teilen mit AWS Organizations zu aktivieren AWS Resource Access Manager

- Folgen Sie den Anweisungen unter [Teilen aktivieren mit AWS Organizations](#) im AWS Resource Access Manager Benutzerhandbuch.

Wenn Sie Probleme mit der gemeinsamen Nutzung von Ressourcen haben, finden Sie weitere Informationen in der Anleitung unter [Gemeinsame Nutzung von Ressourcen für Network Firewall- und DNS-Firewall-Richtlinien](#).

Schritt 6: Zur Verwendung AWS Firewall Manager in Regionen, die standardmäßig deaktiviert sind

Um Firewall Manager in einer Region zu verwenden, die standardmäßig deaktiviert ist, müssen Sie die Region sowohl für das Verwaltungskonto Ihrer AWS Organisation als auch für das Firewall Manager Manager-Standardadministratorkonto aktivieren. Informationen zu Regionen, die standardmäßig deaktiviert sind, und zu deren Aktivierung finden Sie unter [Verwaltung AWS-Regionen](#) in der AWS allgemeinen Referenz.

So aktivieren Sie eine deaktivierte Region

- Folgen Sie sowohl für das Organisationsverwaltungskonto als auch für das Firewall Manager Manager-Standardadministratorkonto den Anweisungen unter [Region aktivieren](#) in der AWS Allgemeinen Referenz.

Nachdem Sie diese Schritte ausgeführt haben, können Sie den Firewall Manager so konfigurieren, dass er mit dem Schutz Ihrer Ressourcen beginnt. Weitere Informationen finden Sie unter [Erste Schritte mit AWS Firewall Manager AWS WAF Richtlinien](#).

Zusammenarbeit mit AWS Firewall Manager Administratoren

Damit können AWS Firewall Manager Sie einen oder mehrere Administratoren haben, die die Firewall-Ressourcen Ihres Unternehmens verwalten können. Wenn Sie mehrere Firewall Manager Manager-Administratoren in Ihrer Organisation verwenden möchten, können Sie für jeden Administrator Bedingungen für den administrativen Geltungsbereich festlegen, um die Ressourcen zu definieren, die er verwalten kann. Dies gibt Ihnen die Flexibilität, innerhalb Ihrer Organisation unterschiedliche Administratorrollen zu haben, und hilft Ihnen, das Prinzip des geringsten Zugriffs beizubehalten. Sie können beispielsweise festlegen, dass ein Administrator eine Reihe von

Organisationseinheiten (OUs) für Ihr Unternehmen verwaltet, während Sie gleichzeitig einen anderen Administrator mit der Verwaltung nur bestimmter Firewall Manager Manager-Richtlinientypen beauftragen. Weitere Informationen zu Organizations und Verwaltungskonten finden Sie unter [AWS Konten in Ihrer Organisation verwalten](#).

Die maximale Anzahl von Administratoren, die Sie pro Organisation haben können, finden Sie unter [AWS Firewall Manager Kontingente](#)

Erste Schritte mit Firewall Manager Manager-Administratoren

Bevor Sie mit der Verwendung von Firewall Manager Manager-Administratoren beginnen, müssen Sie die unter aufgeführten Voraussetzungen erfüllen [AWS Firewall Manager Voraussetzungen](#). In den Voraussetzungen integrieren Sie ein AWS Organizations Unternehmen in Firewall Manager und erstellen ein Standard-Administratorkonto für Firewall Manager. Ein Standard-Administratorkonto ist in der Lage, Firewalls von Drittanbietern zu verwalten, und hat vollen administrativen Umfang.

Administrativer Geltungsbereich

Der administrative Bereich definiert die Ressourcen, die der Firewall Manager Manager-Administrator verwalten kann. Nachdem ein AWS Organizations Verwaltungskonto eine Organisation in Firewall Manager integriert hat, kann das Verwaltungskonto zusätzliche Firewall Manager Manager-Administratoren mit unterschiedlichen Verwaltungsbereichen einrichten. Ein AWS Organizations Verwaltungskonto kann dem Administrator entweder vollen oder eingeschränkten Administratorbereich gewähren. Der vollständige Gültigkeitsbereich gewährt dem Administrator vollen Zugriff auf alle oben genannten Ressourcentypen. Eingeschränkter Geltungsbereich bezieht sich auf die Gewährung von Administratorberechtigungen nur für eine Teilmenge der vorherigen Ressourcen. Es wird empfohlen, Administratoren nur die Berechtigungen zu gewähren, die sie zur Erfüllung der Aufgaben ihrer Rolle benötigen. Sie können eine beliebige Kombination dieser Bedingungen für den administrativen Geltungsbereich auf einen Administrator anwenden:

- Konten oder Organisationseinheiten in Ihrer Organisation, auf die der Administrator Richtlinien anwenden kann.
- Regionen, in denen der Administrator Aktionen ausführen kann.
- Firewall Manager Manager-Richtlinientypen, die der Administrator verwalten kann.

Administratorrollen

In Firewall Manager gibt es zwei Arten von Administratorrollen: einen Standardadministrator und Firewall Manager Manager-Administratoren.

- **Standardadministrator** — Das Verwaltungskonto der Organisation erstellt ein Firewall Manager-Standardadministratorkonto, wenn sie ihre Organisation bei Firewall Manager einbinden und gleichzeitig den Vorgang abschließen [AWS Firewall Manager Voraussetzungen](#). Der Standardadministrator kann Firewalls von Drittanbietern verwalten und verfügt über den vollen administrativen Bereich, befindet sich aber ansonsten auf derselben Peer-Ebene wie andere Administratoren, falls Sie sich für mehrere Administratoren entscheiden.
- **Firewall Manager Manager-Administratoren** — Ein Firewall Manager Manager-Administrator kann die Ressourcen verwalten, die ihm das AWS Organizations Verwaltungskonto in seiner Konfiguration mit administrativem Geltungsbereich zuweist. Die maximale Anzahl von Administratoren, die Sie pro Organisation haben können, finden Sie unter [AWS Firewall Manager Kontingente](#). Bei der Erstellung eines Firewall Manager-Administratorkontos prüft der Dienst, ob es sich bei dem Konto bereits AWS Organizations um einen delegierten Administrator für Firewall Manager innerhalb der Organisation handelt. Wenn nicht, ruft Firewall Manager Organizations auf, um das Konto als delegierten Administrator für Firewall Manager einzurichten. Informationen zu delegierten Administratoren von Organizations finden Sie unter [AWS Organizations Terminologie und Konzepte](#) im AWS Organizations Benutzerhandbuch.

Bestehende Administratoren

Wenn Sie bereits ein Firewall Manager Manager-Kunde sind und bereits einen Administrator eingerichtet haben, dann ist dieser bestehende Administrator der Firewall Manager Manager-Standardadministrator. Es sollte keine Auswirkungen auf Ihren bestehenden Ablauf geben. Wenn Sie weitere Administratoren hinzufügen möchten, können Sie dies tun, indem Sie die Verfahren in diesem Kapitel befolgen.

Firewall Manager Manager-Administratorkonten erstellen, aktualisieren und sperren

Die Verfahren in den folgenden Themen erläutern, wie Sie Firewall Manager Manager-Administratorkonten erstellen, aktualisieren und widerrufen. Nur das Verwaltungskonto einer Organisation kann Firewall Manager-Administratorkonten erstellen und aktualisieren. Nur ein einzelner Firewall Manager Manager-Administrator kann sein eigenes Administratorkonto widerrufen.

Ein Firewall Manager Manager-Administratorkonto erstellen

Das folgende Verfahren beschreibt, wie Sie mit der Firewall Manager Manager-Konsole ein Firewall Manager Manager-Administratorkonto erstellen.

So erstellen Sie ein Firewall Manager Manager-Administratorkonto

1. Melden Sie sich AWS Management Console mit einem vorhandenen AWS Organizations Verwaltungskonto beim Firewall Manager an.
2. Öffnen Sie die Firewall Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>.
3. Wählen Sie im Navigationsbereich Settings (Einstellungen).
4. Wählen Sie Administratorkonto erstellen.
5. Geben Sie im Bereich Details als AWS Konto-ID die AWS ID eines Mitgliedskontos ein, das Sie als Firewall Manager Manager-Administrator hinzufügen möchten.
6. Wählen Sie für den administrativen Bereich eine der folgenden Optionen aus:
 - Vollständig — Dies gibt dem Administrator die Möglichkeit, Richtlinien auf alle Konten und Organisationseinheiten (OUs) innerhalb der Organisation anzuwenden, Maßnahmen in allen Regionen zu ergreifen und alle Firewall Manager Manager-Richtlinientypen anzuwenden, mit Ausnahme von Firewalls von Drittanbietern. Nur der Standardadministrator kann Firewalls von Drittanbietern erstellen und verwalten. Seien Sie vorsichtig, wenn Sie dem Administrator diese Berechtigungsebene gewähren. Im Sinne der geringsten Rechte empfehlen wir, dem Administrator nur die Berechtigungen zu gewähren, die er zur Erfüllung der Aufgaben seiner Rolle benötigt.
 - Eingeschränkt — Wenn Sie einen eingeschränkten Bereich anwenden, konfigurieren Sie unter Administratorbereich konfigurieren die Konten und Organisationseinheiten, Regionen und Richtlinientypen, die das Konto verwalten kann.


Wählen Sie für Konten und Organisationseinheiten die Optionen wie folgt aus:

- Wenn Sie Richtlinien auf alle Konten oder Organisationseinheiten in Ihrer Organisation anwenden möchten, wählen Sie Alle Konten meiner AWS Organisation einbeziehen aus.
- Wenn Sie Richtlinien nur auf bestimmte Konten oder Konten anwenden möchten, die sich in bestimmten AWS Organizations Organisationseinheiten (OUs) befinden, wählen Sie Nur die angegebenen Konten und Organisationseinheiten einbeziehen aus und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie einbeziehen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.
- Wenn Sie Richtlinien für alle Konten oder Organisationseinheiten (OUs) außer für eine bestimmte Gruppe von Konten oder AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Die angegebenen Konten und Organisationseinheiten

ausschließen und alle anderen einbeziehen aus, und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie ausschließen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

Wählen Sie für Regionen die Optionen wie folgt aus:

- Wenn Sie dem Administrator erlauben möchten, Aktionen in allen verfügbaren Regionen durchzuführen, wählen Sie Alle Regionen einbeziehen aus.
- Wenn Sie möchten, dass der Administrator Aktionen nur in bestimmten Regionen ausführt, wählen Sie Nur die angegebenen Regionen einbeziehen aus und geben Sie dann die Regionen an, die Sie einbeziehen möchten.

 Note

Um eine Region einzubeziehen, die standardmäßig deaktiviert ist, müssen Sie die Region sowohl für das AWS Organizations Organisationsverwaltungskonto als auch für das Standard-Verwaltungskonto aktivieren. Informationen zum Aktivieren von Regionen für ein Konto finden Sie unter [Aktivieren einer Region](#) in der Allgemeine Amazon Web Services-Referenz.

Wählen Sie für Richtlinientypen die folgenden Optionen aus:

- Wenn Sie dem Administrator die Verwaltung aller Richtlinientypen ermöglichen möchten, wählen Sie Alle Richtlinientypen einbeziehen aus.
 - Wenn Sie möchten, dass der Administrator nur bestimmte Richtlinientypen verwaltet, wählen Sie Nur die angegebenen Richtlinientypen einbeziehen aus und geben Sie dann die Richtlinientypen an, die Sie einbeziehen möchten.
7. Wählen Sie Administratorkonto erstellen aus, um das Administratorkonto zu erstellen. Nach der Erstellung ruft Firewall Manager an, AWS Organizations um festzustellen, ob der Administrator bereits ein delegierter Administrator für Ihr Unternehmen ist. Andernfalls weist Firewall Manager das Konto als delegierten Administrator zu. Informationen zu delegierten Administratoren in Organizations finden Sie unter [AWS Organizations Terminologie und Konzepten](#) im AWS Organizations Benutzerhandbuch.

Wenn Sie den eingeschränkten administrativen Bereich verwenden, bewertet Firewall Manager automatisch alle neuen Ressourcen anhand Ihrer Einstellungen. Wenn Sie beispielsweise nur bestimmte Konten angeben, wendet Firewall Manager die Richtlinie nicht auf neue Konten an. Ein weiteres Beispiel: Wenn Sie eine Organisationseinheit hinzufügen und der Organisationseinheit oder einer ihrer untergeordneten Organisationseinheiten ein Konto hinzufügen, nimmt Firewall Manager das Konto automatisch in den administrativen Bereich auf.

Aktualisierung eines Firewall Manager Manager-Administratorkontos

Das folgende Verfahren beschreibt, wie Sie ein Firewall Manager Manager-Administratorkonto mithilfe der Firewall Manager Manager-Konsole aktualisieren.

Note

Um den Geltungsbereich eines Administrators so zu aktualisieren, dass er eine Region einschließt, die standardmäßig deaktiviert ist, müssen Sie die Region sowohl für das AWS Organizations Organisationsverwaltungskonto als auch für das Standard-Administratorkonto aktivieren. Informationen zur Aktivierung von Regionen für ein Konto finden Sie unter [Aktivieren einer Region](#) in der Allgemeine Amazon Web Services-Referenz.

So aktualisieren Sie ein Administratorkonto (Konsole)

1. Melden Sie sich AWS Management Console mit einem vorhandenen AWS Organizations Verwaltungskonto beim Firewall Manager an.
2. Öffnen Sie die Firewall Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>.
3. Wählen Sie im Navigationsbereich Settings (Einstellungen).
4. Wählen Sie in der Administratortabelle von Firewall Manager das Konto aus, das Sie aktualisieren möchten.
5. Wählen Sie Bearbeiten aus, um die Details des Administratorkontos zu ändern. Sie können die Konto-ID nicht ändern.
6. Wählen Sie Speichern, um Ihre Änderungen zu speichern.


Widerrufen eines Administratorkontos

Das folgende Verfahren beschreibt, wie Sie ein Firewall Manager Manager-Administratorkonto widerrufen. Wenn Sie der Standardadministrator sind, müssen zunächst alle Firewall Manager

Manager-Administratorkonten in Ihrer Organisation ihre eigenen Konten sperren, bevor Sie Ihr Konto sperren können. Gehen Sie wie folgt vor, um ein Administratorkonto zu widerrufen

Um ein Administratorkonto zu widerrufen (Konsole)

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie im Bereich Administratorkonto die Option Administratorkonto widerrufen aus, um Ihr Konto zu widerrufen.

 **Important**

Wenn Sie einem Administratorkonto Administratorrechte entziehen, werden alle von diesem Konto erstellten Firewall Manager Manager-Richtlinien gelöscht.


Ändern des Standard-Administratorkontos

Sie können nur ein Konto in einer Organisation als Standard-Firewall Manager-Administratorkonto festlegen. Das Standard-Administratorkonto folgt dem Prinzip: zuerst rein, zuletzt raus. Um ein anderes Standard-Administratorkonto festzulegen, muss jedes einzelne Administratorkonto zunächst sein eigenes Konto sperren. Anschließend kann der bestehende Standardadministrator sein eigenes Konto sperren, wodurch die Organisation auch aus Firewall Manager ausgegliedert wird. Wenn ein Administrator sein Konto sperrt, werden alle von diesem Konto erstellten Firewall Manager Manager-Richtlinien gelöscht. Um ein neues Standard-Administratorkonto festzulegen, müssen Sie sich anschließend mit dem AWS Organizations Verwaltungskonto bei Firewall Manager anmelden, um ein neues Administratorkonto festzulegen. Gehen Sie wie folgt vor, um das Standard-Administratorkonto für eine Organisation zu ändern.

Um das Standard-Administratorkonto zu ändern


1. Melden Sie sich AWS Management Console mit einem vorhandenen AWS Organizations Verwaltungskonto beim Firewall Manager an.
2. Öffnen Sie die Firewall Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>.

3. Wählen Sie im Navigationsbereich Settings (Einstellungen).
4. Geben Sie die ID des Kontos ein, das Sie als Firewall Manager Manager-Administrator verwenden möchten.

 Note

Dieses Konto ist berechtigt, Firewall Manager Manager-Richtlinien für alle Konten in Ihrer Organisation zu erstellen und zu verwalten.

5. Wählen Sie Administratorkonto erstellen aus.
6. Geben Sie die AWS ID des Kontos ein, das Sie als Firewall Manager Manager-Administrator verwenden möchten.

 Note

Diesem Konto wird der volle Administratorbereich zugewiesen. Vollständiger administrativer Geltungsbereich bedeutet, dass dieses Konto Richtlinien auf alle Konten und Organisationseinheiten (OUs) innerhalb der Organisation anwenden, Aktionen in allen Regionen ergreifen und alle Firewall Manager Manager-Richtlinientypen verwalten kann.

7. Wählen Sie Administratorkonto erstellen, um das Standard-Administratorkonto zu erstellen.

Änderungen an einem Administratorkonto disqualifizieren

Einige Änderungen an einem Administratorkonto können dazu führen, dass es kein Administratorkonto mehr bleibt.

In diesem Abschnitt werden die Änderungen beschrieben, die ein Administratorkonto disqualifizieren können, AWS und wie Firewall Manager mit diesen Änderungen umgeht.

Das Konto wurde aus der Organisation entfernt in AWS Organizations

Wenn das AWS Firewall Manager Administratorkonto aus der Organisation entfernt wird AWS Organizations, kann es keine Richtlinien mehr für die Organisation verwalten. Firewall Manager führt eine der folgenden Aktionen aus:

- Konto ohne Richtlinien — Wenn das Firewall Manager-Administratorkonto keine Firewall Manager Richtlinien hat, sperrt Firewall Manager das Administratorkonto.
- Konto mit Firewall Manager-Richtlinien — Wenn das Firewall Manager Administratorkonto über Firewall Manager Richtlinien verfügt, sendet Ihnen Firewall Manager eine E-Mail, um Sie über die Situation zu informieren und Ihnen Optionen vorzuschlagen, die Sie mit Hilfe Ihres AWS Kundenbetreuers wählen können.

Konto geschlossen

Wenn Sie das Konto schließen, das Sie für den AWS Firewall Manager Administrator verwenden, AWS und Firewall Manager die Schließung wie folgt handhabt:

- AWS widerruft den Administratorzugriff des Kontos über Firewall Manager und Firewall Manager deaktiviert alle Richtlinien, die vom Administratorkonto verwaltet wurden. Die Schutzmaßnahmen, die durch diese Richtlinien bereitgestellt wurden, wurden unternehmensweit aufgehoben.
- AWS bewahrt die Firewall Manager Richtlinien für das Konto 90 Tage ab dem Datum des Inkrafttretens der Schließung des Administratorkontos auf. Während dieses Zeitraums von 90 Tagen können Sie das geschlossene Konto erneut öffnen.
 - Wenn Sie das geschlossene Konto innerhalb von 90 Tagen erneut öffnen, AWS weist es dem Konto erneut als Firewall Manager Administrator zu und stellt die Firewall Manager Richtlinien für das Konto wieder her.
 - Andernfalls werden am Ende des 90-Tage-Zeitraums alle Firewall Manager Richtlinien für das Konto AWS dauerhaft gelöscht.

Erste Schritte mit AWS Firewall Manager Richtlinien

Sie können sie verwenden AWS Firewall Manager , um eine Reihe verschiedener Arten von Sicherheitsrichtlinien zu aktivieren. Die Schritte zum Einrichten sind dafür jeweils etwas unterschiedlich.

Themen

- [Erste Schritte mit AWS Firewall Manager AWS WAF Richtlinien](#)
- [Erste Schritte mit AWS Firewall Manager AWS Shield Advanced Richtlinien](#)
- [Erste Schritte mit AWS Firewall Manager Amazon VPC-Sicherheitsgruppenrichtlinien](#)
- [Erste Schritte mit AWS Firewall Manager AWS Network Firewall Richtlinien](#)

- [Erste Schritte mit AWS Firewall Manager DNS-Firewall-Richtlinien](#)
- [Erste Schritte mit den Cloud-Firewall-Richtlinien der nächsten Generation von AWS Firewall Manager Palo Alto Networks](#)
- [Erste Schritte mit den AWS Firewall Manager Fortigate CNF-Richtlinien](#)

Erste Schritte mit AWS Firewall Manager AWS WAF Richtlinien

Um AWS WAF Regeln in Ihrer gesamten Organisation AWS Firewall Manager zu aktivieren, führen Sie die folgenden Schritte nacheinander aus.

Themen

- [Schritt 1: Erfüllen der Voraussetzungen](#)
- [Schritt 2: AWS WAF Richtlinie erstellen und anwenden](#)
- [Schritt 3: Bereinigen](#)

Schritt 1: Erfüllen der Voraussetzungen

Mehrere Schritte sind zur Vorbereitung Ihres Kontos auf AWS Firewall Manager zwingend erforderlich. Diese Schritte werden in [AWS Firewall Manager Voraussetzungen](#) beschrieben. Erfüllen Sie alle Voraussetzungen, bevor Sie mit [Schritt 2: AWS WAF Richtlinie erstellen und anwenden](#) fortfahren.

Schritt 2: AWS WAF Richtlinie erstellen und anwenden

Eine Firewall Manager AWS WAF Manager-Richtlinie enthält die Regelgruppen, die Sie auf Ihre Ressourcen anwenden möchten. Firewall Manager erstellt in jedem Konto, auf das Sie die Richtlinie anwenden, eine Firewall Manager Manager-Web-ACL. Die einzelnen Accountmanager können neben den hier definierten Regelgruppen der resultierenden Web-ACL Regeln und Regelgruppen hinzufügen. Informationen zu den AWS WAF Richtlinien von Firewall Manager finden Sie unter [AWS WAF Richtlinien](#).

So erstellen Sie eine Firewall Manager AWS WAF Manager-Richtlinie (Konsole)

Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

1. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
2. Wählen Sie Richtlinie erstellen aus.
3. Wählen Sie unter Policy type (Richtlinientyp) die Option AWS WAF.
4. Wählen Sie für Region eine AWS-Region. Um CloudFront Amazon-Distributionen zu schützen, wählen Sie Global.

Um Ressourcen in mehreren Regionen (außer CloudFront Verteilungen) zu schützen, müssen Sie separate Firewall Manager Manager-Richtlinien für jede Region erstellen.

5. Wählen Sie Weiter aus.
6. Geben Sie als Richtliniennamen einen aussagekräftigen Namen ein. Firewall Manager nimmt den Richtliniennamen in die Namen der Web-ACLs auf, die er verwaltet. Auf die Web-ACL-Namen FMManagedWebACLV2- folgten der Richtliniennamen, den Sie hier eingeben-, und der Zeitstempel für die Erstellung der Web-ACL in UTC-Millisekunden. z. B. FMManagedWebACLV2-MyWAFPolicyName-1621880374078.

 **Important**

Web-ACL-Namen können sich nach der Erstellung nicht ändern. Wenn Sie den Namen Ihrer Richtlinie aktualisieren, aktualisiert Firewall Manager den zugehörigen Web-ACL-Namen nicht. Damit Firewall Manager eine Web-ACL mit einem anderen Namen erstellt, müssen Sie eine neue Richtlinie erstellen.

7. Wählen Sie unter Policy rules (Richtlinienregeln) für First rule groups (Erste Regelgruppen) die Option Add rule groups (Regelgruppen hinzufügen) aus. Erweitern Sie die AWS verwalteten Regelgruppen. Aktivieren Sie unter Core rule set (Kernregelsatz) Add to web ACL (Zu Web-ACL hinzufügen). Bei AWS bekannten fehlerhaften Eingaben aktivieren Sie die Option Zur Web-ACL hinzufügen. Wählen Sie Add rules (Regeln hinzufügen) aus

Wählen Sie unter Last rule groups (Letzte Regelgruppen) die Option Add rule groups (Regelgruppen hinzufügen) aus. Erweitern Sie die AWS verwalteten Regelgruppen und aktivieren Sie für die Amazon IP-Reputationsliste die Option Zur Web-ACL hinzufügen. Wählen Sie Add rules (Regeln hinzufügen) aus

Wählen Sie unter Erste Regelgruppen die Option Kernregelsatz und dann Nach unten verschieben aus. AWS WAF wertet Webanfragen anhand der Regelgruppe mit AWS bekannten fehlerhaften Eingaben aus, bevor sie anhand des Core-Regelsatzes ausgewertet werden.

Wenn Sie möchten, können Sie mit der Konsole auch Ihre eigenen AWS WAF Regelgruppen erstellen. AWS WAF Alle von Ihnen erstellten Regelgruppen werden unter Your rule groups (Ihre Regelgruppen) auf der Seite Describe policy: Add rule groups (Richtlinie beschreiben: Regelgruppen hinzufügen) angezeigt.

Die ersten und letzten AWS WAF Regelgruppen, die Sie über Firewall Manager verwalten, haben Namen `POSTFMMManaged-`, die mit dem `PREFMManaged-` Namen der Firewall Manager Manager-Richtlinie und dem Zeitstempel für die Erstellung der Regelgruppe in UTC-Millisekunden beginnen bzw. darauf folgen. z. B. `PREFMManaged-MyWAFPolicyName-1621880555123`.

8. Lassen Sie die Standardaktion für die Web-ACL bei Allow (Zulassen).
9. Lassen Sie die Policy action (Richtlinienaktion) bei der Standardeinstellung, um nicht konforme Ressourcen nicht automatisch zu korrigieren. Sie können die Option später ändern.
10. Wählen Sie Weiter aus.
11. Für den Policy scope (Richtlinienbereich) geben Sie die Einstellungen für die Konten, Ressourcentypen und das Tagging an, die die Ressourcen identifizieren, auf die Sie die Richtlinie anwenden möchten. Verlassen Sie für dieses Tutorial die Einstellungen AWS-Konten und Ressourcen und wählen Sie einen oder mehrere Ressourcentypen aus.
12. Wählen Sie Weiter aus.
13. Für Policy-Tags können Sie beliebige Identifizierungs-Tags für die Firewall Manager AWS WAF Manager-Richtlinie hinzufügen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#). Für dieses Tutorial können Sie dies unberücksichtigt lassen.
14. Wählen Sie Weiter aus.
15. Überprüfen Sie die neue Richtlinie. Sie können Änderungen vornehmen, indem Sie Edit (Bearbeiten) in dem Bereich wählen, den Sie ändern möchten. Dadurch kehren Sie zum entsprechenden Schritt im Erstellungsassistenten zurück. Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen).

Schritt 3: Bereinigen

Um zu hohe Gebühren zu vermeiden, löschen Sie alle unnötigen Richtlinien und Ressourcen.

So löschen Sie eine Richtlinie (Konsole)

1. Wählen Sie auf der AWS Firewall Manager Richtlinienseite das Optionsfeld neben dem Richtliniennamen und wählen Sie dann Löschen aus.
2. Wählen Sie im Bestätigungsfeld Delete (Löschen) die Option Delete all policy resources (Alle Richtlinienressourcen löschen) aus und wählen Sie dann erneut Delete (Löschen).

AWS WAF entfernt die Richtlinie und alle zugehörigen Ressourcen, wie Web-ACLs, die sie in Ihrem Konto erstellt hat. Es kann einige Minuten dauern, bis die Änderungen an alle Konten weitergegeben werden.

Erste Schritte mit AWS Firewall ManagerAWS Shield Advanced Richtlinien

Sie können sie verwenden AWS Firewall Manager , um AWS Shield Advanced Schutzmaßnahmen in Ihrer gesamten Organisation zu aktivieren.

Important

Firewall Manager unterstützt Amazon Route 53 oder nicht AWS Global Accelerator. Wenn Sie diese Ressourcen mit Shield Advanced schützen müssen, können Sie keine Firewall Manager Richtlinie verwenden. Folgen Sie stattdessen den Anweisungen in [AWS Shield Advanced Schutz für Ressourcen hinzufügen AWS](#).

Um den Firewall Manager zur Aktivierung des Shield Advanced-Schutzes zu verwenden, führen Sie die folgenden Schritte nacheinander aus.

Themen

- [Schritt 1: Erfüllen der Voraussetzungen](#)
- [Schritt 2: Erstellen und Anwenden einer Shield Advanced-Richtlinie](#)
- [Schritt 3: \(Optional\) autorisieren Sie das Shield Response Team \(SRT\)](#)
- [Schritt 4: Amazon SNS SNS-Benachrichtigungen und CloudWatch Amazon-Alarme konfigurieren](#)

Schritt 1: Erfüllen der Voraussetzungen

Mehrere Schritte sind zur Vorbereitung Ihres Kontos auf AWS Firewall Manager zwingend erforderlich. Diese Schritte werden in [AWS Firewall Manager Voraussetzungen](#) beschrieben. Erfüllen

Sie alle Voraussetzungen, bevor Sie mit [Schritt 2: Erstellen und Anwenden einer Shield Advanced-Richtlinie](#) fortfahren.

Schritt 2: Erstellen und Anwenden einer Shield Advanced-Richtlinie

Nachdem Sie die Voraussetzungen erfüllt haben, erstellen Sie eine AWS Firewall Manager Shield Advanced-Richtlinie. Eine Firewall Manager Shield Advanced-Richtlinie enthält die Konten und Ressourcen, die Sie mit Shield Advanced schützen möchten.

Important

Firewall Manager unterstützt Amazon Route 53 oder nicht AWS Global Accelerator. Wenn Sie diese Ressourcen mit Shield Advanced schützen müssen, können Sie keine Firewall Manager Manager-Richtlinie verwenden. Folgen Sie stattdessen den Anweisungen in [AWS Shield Advanced Schutz für Ressourcen hinzufügen AWS](#).

So erstellen Sie eine Firewall Manager Shield Advanced-Richtlinie (Konsole)


1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie als Richtlinientyp Shield Advanced aus.

Um eine Shield Advanced-Richtlinie zu erstellen, muss Ihr Firewall Manager Manager-Administratorkonto Shield Advanced abonniert haben. Wenn Sie kein Abonnement eingerichtet haben, werden Sie dazu aufgefordert. [Informationen zu den Kosten für ein Abonnement finden Sie unter AWS Shield Advanced Preise](#).

 Note

Sie müssen nicht jedes Mitgliedskonto manuell für Shield Advanced abonnieren. Firewall Manager erledigt dies für Sie, wenn er die Richtlinie erstellt. Jedes Konto muss weiterhin für Firewall Manager und Shield Advanced abonniert bleiben, um die Ressourcen im Konto weiterhin zu schützen.

5. Wählen Sie für Region eine AWS-Region. Um CloudFront Amazon-Ressourcen zu schützen, wählen Sie Global.

Um Ressourcen in mehreren Regionen (außer CloudFront Ressourcen) zu schützen, müssen Sie separate Firewall Manager Manager-Richtlinien für jede Region erstellen.

6. Wählen Sie Weiter aus.
7. Geben Sie unter Name einen aussagekräftigen Namen ein.
8. (Nur globale Region) Bei Richtlinien für globale Regionen können Sie wählen, ob Sie die automatische DDoS-Abwehr auf Anwendungsebene mit Shield Advanced verwalten möchten. Behalten Sie für dieses Tutorial die Standardeinstellung Ignorieren für diese Auswahl bei.
9. Wählen Sie unter Richtlinienaktion die Option aus, die nicht automatisch behoben wird.
10. Wählen Sie Weiter aus.
11. AWS-Konten Mit dieser Richtlinie können Sie den Geltungsbereich Ihrer Richtlinie einschränken, indem Sie Konten angeben, die ein- oder ausgeschlossen werden sollen. In diesem Tutorial wählen Sie Include all accounts under my organization (Alle Konten in meiner Organisation einschließen).
12. Wählen Sie die Ressourcentypen aus, die geschützt werden sollen.

Firewall Manager unterstützt Amazon Route 53 oder nicht AWS Global Accelerator. Wenn Sie diese Ressourcen mit Shield Advanced schützen müssen, können Sie keine Firewall Manager Manager-Richtlinie verwenden. Folgen Sie stattdessen den Anweisungen von Shield Advanced unter [AWS Shield Advanced Schutz für Ressourcen hinzufügen AWS](#).

13. Wenn Sie nur Ressourcen mit bestimmten Tags schützen oder Ressourcen mit bestimmten Tags ausschließen möchten, wählen Sie „Tags zum Ein-/Ausschließen von Ressourcen verwenden“ aus, geben Sie die durch Kommas getrennten Tags ein und wählen Sie dann entweder „Einschließen“ oder „Ausschließen“. Sie können nur eine Option auswählen.

Wenn Sie mehr als ein Tag eingeben und eine Ressource über eines dieser Tags verfügt, wird dies als Übereinstimmung betrachtet.

Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).

14. Wählen Sie Weiter aus.
15. Fügen Sie für Policy-Tags alle Identifizierungs-Tags hinzu, die Sie für die Firewall Manager Manager-Richtlinie benötigen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).
16. Wählen Sie Weiter aus.
17. Überprüfen Sie die neue Richtlinie. Um Änderungen vorzunehmen, wählen Sie Previous (Zurück). Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen).

Fahren Sie fort mit [Schritt 3: \(Optional\) autorisieren Sie das Shield Response Team \(SRT\)](#).

Schritt 3: (Optional) autorisieren Sie das Shield Response Team (SRT)

Einer der Vorteile von AWS Shield Advanced ist die Unterstützung durch das Shield Response Team (SRT). [Wenn Sie von einem potenziellen DDoS-Angriff betroffen sind, können Sie sich an das AWS Support Center wenden](#). Falls erforderlich, leitet das Support Center Ihr Problem an das SRT weiter. Das SRT hilft Ihnen bei der Analyse der verdächtigen Aktivitäten und unterstützt Sie bei der Behebung des Problems. Diese Abhilfemaßnahme beinhaltet häufig die Erstellung oder Aktualisierung von AWS WAF Regeln und Web-ACLs in Ihrem Konto. Das SRT kann Ihre AWS WAF Konfiguration überprüfen und AWS WAF Regeln und Web-ACLs für Sie erstellen oder aktualisieren. Das Team benötigt dafür jedoch Ihre Genehmigung. Wir empfehlen, dass Sie dem SRT im Rahmen der Einrichtung AWS Shield Advanced proaktiv die erforderliche Autorisierung erteilen. Die frühzeitige Autorisierung verhindert Verzögerungen bei der Problembekämpfung im Fall eines tatsächlichen Angriffs.

Sie autorisieren und kontaktieren das SRT auf Kontoebene. Das heißt, der Kontoinhaber, nicht der Firewall Manager Manager-Administrator, muss die folgenden Schritte ausführen, um das SRT zur Abwehr potenzieller Angriffe zu autorisieren. Der Firewall Manager Manager-Administrator kann die SRT nur für Konten autorisieren, deren Eigentümer er ist. Ebenso kann sich nur der Kontoinhaber an das SRT wenden, um Support zu erhalten.

Note

Um die Dienste des SRT nutzen zu können, müssen Sie den [Business Support Plan](#) oder den [Enterprise Support Plan](#) abonniert haben.

Um das SRT zu autorisieren, potenzielle Angriffe in Ihrem Namen abzuwehren, folgen Sie den Anweisungen unter [Unterstützung durch das Shield Response Team \(SRT\)](#). Sie können den SRT-Zugriff und die Berechtigungen jederzeit ändern, indem Sie dieselben Schritte ausführen.

Fahren Sie fort mit [Schritt 4: Amazon SNS SNS-Benachrichtigungen und CloudWatch Amazon-Alarme konfigurieren](#).

Schritt 4: Amazon SNS SNS-Benachrichtigungen und CloudWatch Amazon-Alarme konfigurieren

Sie können mit diesem Schritt fortfahren, ohne Amazon SNS SNS-Benachrichtigungen oder CloudWatch -Alarme zu konfigurieren. Die Konfiguration dieser Alarme und Benachrichtigungen erhöht jedoch Ihren Überblick über mögliche DDoS-Ereignisse erheblich.

Mit Amazon SNS können Sie Ihre geschützten Ressourcen auf potenzielle DDoS-Aktivitäten überwachen. Um Benachrichtigungen über mögliche Angriffe zu erhalten, erstellen Sie für jede Region ein Amazon SNS SNS-Thema.

Um ein Amazon SNS SNS-Thema in Firewall Manager (Konsole) zu erstellen

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich unter AWS FMS die Option Einstellungen aus.
3. Wählen Sie Create new topic (Neues Thema erstellen).
4. Geben Sie einen Themennamen ein.

5. Geben Sie eine E-Mail-Adresse ein, an die die Amazon SNS SNS-Nachrichten gesendet werden, und wählen Sie dann E-Mail-Adresse hinzufügen.
6. Wählen Sie Update SNS configuration (SNS-Konfiguration aktualisieren).

CloudWatch Amazon-Alarme konfigurieren

Shield Advanced zeichnet Kennzahlen zur Erkennung, Abwehr und wichtigsten Mitwirkenden auf CloudWatch , die Sie überwachen können. Weitere Informationen finden Sie unter [AWS Shield Advanced Metriken](#) CloudWatch verursacht zusätzliche Kosten. CloudWatch Die Preise finden Sie unter [CloudWatch Amazon-Preise](#).

Um einen CloudWatch Alarm zu erstellen, folgen Sie den Anweisungen unter [Amazon CloudWatch Alarms verwenden](#). Standardmäßig ist Shield Advanced so konfiguriert, CloudWatch dass Sie nach nur einem Hinweis auf ein potenzielles DDoS-Ereignis gewarnt werden. Bei Bedarf können Sie die CloudWatch Konsole verwenden, um diese Einstellung so zu ändern, dass Sie erst benachrichtigt werden, wenn mehrere Indikatoren erkannt werden.

Note

Zusätzlich zu den Alarmen können Sie auch ein CloudWatch Dashboard verwenden, um potenzielle DDoS-Aktivitäten zu überwachen. Das Dashboard sammelt und verarbeitet Rohdaten von Shield Advanced in lesbare Metriken, die nahezu in Echtzeit verfügbar sind. Sie können Statistiken in Amazon verwenden CloudWatch , um sich einen Überblick über die Leistung Ihrer Webanwendung oder Ihres Dienstes zu verschaffen. Weitere Informationen finden Sie unter [Was steht CloudWatch](#) im CloudWatch Amazon-Benutzerhandbuch. Anweisungen zum Erstellen eines CloudWatch Dashboards finden Sie unter [Überwachung mit Amazon CloudWatch](#). Informationen zu bestimmten Shield Advanced-Metriken, die Sie Ihrem Dashboard hinzufügen können, finden Sie unter [AWS Shield Advanced Metriken](#).

Wenn Sie Ihre Shield Advanced-Konfiguration abgeschlossen haben, machen Sie sich mit Ihren Optionen für die Anzeige von Ereignissen unter vertraut [Einblick in DDoS-Ereignisse](#).

Erste Schritte mit AWS Firewall Manager Amazon VPC-Sicherheitsgruppenrichtlinien

Um Amazon VPC-Sicherheitsgruppen in Ihrer Organisation AWS Firewall Manager zu aktivieren, führen Sie die folgenden Schritte nacheinander aus.

Themen

- [Schritt 1: Erfüllen der Voraussetzungen](#)
- [Schritt 2: Erstellen Sie eine Amazon VPC-Sicherheitsgruppe zur Verwendung in Ihrer Richtlinie](#)
- [Schritt 3: Eine gemeinsame Sicherheitsgruppenrichtlinie erstellen und anwenden](#)

Schritt 1: Erfüllen der Voraussetzungen

Mehrere Schritte sind zur Vorbereitung Ihres Kontos auf AWS Firewall Manager zwingend erforderlich. Diese Schritte werden in [AWS Firewall Manager Voraussetzungen](#) beschrieben. Erfüllen Sie alle Voraussetzungen, bevor Sie mit [Schritt 2: Erstellen Sie eine Amazon VPC-Sicherheitsgruppe zur Verwendung in Ihrer Richtlinie](#) fortfahren.

Schritt 2: Erstellen Sie eine Amazon VPC-Sicherheitsgruppe zur Verwendung in Ihrer Richtlinie

In diesem Schritt erstellen Sie eine Sicherheitsgruppe, die Sie mithilfe von Firewall Manager unternehmensweit anwenden können.

Note

In diesem Tutorial wenden Sie Ihre Sicherheitsgruppenrichtlinie nicht auf die Ressourcen in Ihrer Organisation an. Sie erstellen einfach die Richtlinie und sehen, was passieren würde, wenn Sie die Sicherheitsgruppe der Richtlinie auf Ihre Ressourcen anwenden würden. Sie tun dies, indem Sie die automatische Korrektur für die Richtlinie deaktivieren.

Wenn Sie bereits eine allgemeine Sicherheitsgruppe definiert haben, überspringen Sie diesen Schritt und fahren Sie mit [Schritt 3: Eine gemeinsame Sicherheitsgruppenrichtlinie erstellen und anwenden](#) fort.

So erstellen Sie eine Sicherheitsgruppe zur Verwendung in einer allgemeinen Sicherheitsgruppenrichtlinie von Firewall Manager

- Erstellen Sie eine Sicherheitsgruppe, die Sie auf alle Konten und Ressourcen in Ihrer Organisation anwenden können. Folgen Sie dabei den Anweisungen unter [Sicherheitsgruppen für Ihre VPC](#) im [Amazon VPC-Benutzerhandbuch](#).

Weitere Informationen zu den Optionen für Sicherheitsgruppenregeln finden Sie unter [Referenz zu Sicherheitsgruppenregeln](#).

Sie können nun mit [Schritt 3: Eine gemeinsame Sicherheitsgruppenrichtlinie erstellen und anwenden](#) fortfahren.

Schritt 3: Eine gemeinsame Sicherheitsgruppenrichtlinie erstellen und anwenden

Nachdem Sie die Voraussetzungen erfüllt haben, erstellen Sie eine AWS Firewall Manager gemeinsame Sicherheitsgruppenrichtlinie. Eine gemeinsame Sicherheitsgruppenrichtlinie bietet eine zentral gesteuerte Sicherheitsgruppe für Ihr gesamtes AWS Unternehmen. Sie definiert auch die Ressourcen AWS-Konten und Ressourcen, für die die Sicherheitsgruppe gilt. Zusätzlich zu den allgemeinen Sicherheitsgruppenrichtlinien unterstützt Firewall Manager Sicherheitsgruppenrichtlinien zur Inhaltsüberwachung, um die in Ihrer Organisation verwendeten Sicherheitsgruppenregeln zu verwalten, und Sicherheitsgruppenrichtlinien zur Nutzungsüberwachung, um ungenutzte und redundante Sicherheitsgruppen zu verwalten. Weitere Informationen finden Sie unter [Sicherheitsgruppenrichtlinien](#).

Für dieses Tutorial erstellen Sie eine gemeinsame Sicherheitsgruppenrichtlinie und legen deren Aktion so fest, dass sie nicht automatisch korrigiert wird. Auf diese Weise können Sie sehen, welche Auswirkungen die Richtlinie hätte, ohne Änderungen an Ihrer AWS Organisation vorzunehmen.

So erstellen Sie eine allgemeine Sicherheitsgruppenrichtlinie für Firewall Manager (Konsole)

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wenn Sie die Voraussetzungen nicht erfüllen, zeigt die Konsole Anweisungen zum Beheben vorliegender Problemen an. Folgen Sie den Anweisungen und kehren Sie dann zu diesem Schritt zurück, um eine gemeinsame Sicherheitsgruppenrichtlinie zu erstellen.

4. Wählen Sie Richtlinie erstellen aus.
5. Wählen Sie für Policy type (Richtlinientyp) die Option Security group (Sicherheitsgruppe).
6. Wählen Sie für Security group policy type (Sicherheitsgruppenrichtlinientyp) die Option Common security groups (Gemeinsame Sicherheitsgruppen) aus.
7. Wählen Sie für Region eine AWS-Region.
8. Wählen Sie Weiter aus.
9. Geben Sie als Richtliniennamen einen aussagekräftigen Namen ein.
10. Mit Policy rules (Richtlinienregeln) können Sie festlegen, wie die Sicherheitsgruppen in dieser Richtlinie angewendet und verwaltet werden. Lassen Sie die Optionen für dieses Tutorial deaktiviert.
11. Wählen Sie Add primary security group (Primäre Sicherheitsgruppe hinzufügen), wählen Sie die Sicherheitsgruppe aus, die Sie für dieses Tutorial erstellt haben, und wählen Sie Add security group (Sicherheitsgruppe hinzufügen) aus.
12. Wählen Sie für Policy action (Richtlinienaktion) Identify resources that don't comply with the policy rules, but don't auto remediate (Ressourcen identifizieren, die nicht mit den Richtlinienregeln übereinstimmen, aber nicht automatisch korrigieren).
13. Wählen Sie Weiter aus.
14. AWS-Konten Mit der Option „von dieser Richtlinie betroffen“ können Sie den Geltungsbereich Ihrer Richtlinie einschränken, indem Sie Konten angeben, die ein- oder ausgeschlossen werden sollen. In diesem Tutorial wählen Sie Include all accounts under my organization (Alle Konten in meiner Organisation einschließen).
15. Wählen Sie unter Ressourcentyp je nach den Ressourcen, die Sie für Ihre AWS Organisation definiert haben, einen oder mehrere Typen aus.
16. Mit Resources (Ressourcen) können Sie den Geltungsbereich Ihrer Richtlinie einschränken, indem Sie Ressourcen-Tags für die Einbeziehung oder den Ausschluss angeben. Um Tagging zu verwenden, müssen Sie zuerst Ihre Ressourcen markieren. Weitere Informationen zum Kennzeichnen Ihrer Ressourcen finden Sie unter [Arbeiten mit Tag-Editor](#). Wählen Sie für dieses Tutorial Include all resources that match the selected resource type (Alle Ressourcen einschließen, die dem ausgewählten Ressourcentyp entsprechen).
17. Wählen Sie Weiter aus.
18. Überprüfen Sie Ihre Richtlinieneinstellungen. Stellen Sie sicher, dass Policy actions (Richtlinienaktionen) auf Identify resources that don't comply with the policy rules, but don't auto remediate (Ressourcen identifizieren, die nicht mit den Richtlinienregeln übereinstimmen,

aber nicht automatisch korrigieren) festgelegt ist. Auf diese Weise können Sie die Änderungen überprüfen, die Ihre Richtlinie hätte, ohne Änderungen zu diesem Zeitpunkt vorzunehmen.

19. Wählen Sie Richtlinie erstellen aus.

Im Bereich AWS Firewall Manager Richtlinien sollte Ihre Richtlinie aufgeführt sein. Sie wird wahrscheinlich unter den Kontoüberschriften als Pending (Ausstehend) angezeigt. Es wird außerdem angegeben, dass die Automatic remediation (Automatische Korrektur) deaktiviert ist. Die Erstellung einer Richtlinie kann mehrere Minuten dauern. Nachdem der Status Pending (Ausstehend) durch die Kontenanzahl ersetzt wurde, können Sie den Richtliniennamen auswählen, um den Compliance-Status der Konten und Ressourcen zu untersuchen. Weitere Informationen finden Sie unter [Compliance-Informationen für eine AWS Firewall Manager Richtlinie anzeigen](#)

20. Wenn Sie die für dieses Tutorial erstellte Richtlinie nicht beibehalten möchten, wählen Sie den Richtliniennamen aus, wählen Sie Delete (Löschen) und anschließend Clean up resources created by this policy (Ressourcen bereinigen, die von dieser Richtlinie erstellt wurden) aus und wählen Sie schließlich Delete (Löschen) aus.

Weitere Informationen zu den Sicherheitsgruppenrichtlinien von Firewall Manager finden Sie unter [Sicherheitsgruppenrichtlinien](#).

Erste Schritte mit AWS Firewall ManagerAWS Network Firewall Richtlinien

Um eine AWS Network Firewall in Ihrem Unternehmen AWS Firewall Manager zu aktivieren, führen Sie die folgenden Schritte nacheinander aus. Informationen zu den Netzwerk-Firewall-Richtlinien von Firewall Manager finden Sie unter [AWS Network Firewall Richtlinien](#).

Themen

- [Schritt 1: Erfüllen Sie die allgemeinen Voraussetzungen](#)
- [Schritt 2: Erstellen Sie eine Netzwerk-Firewall-Regelgruppe zur Verwendung in Ihrer Richtlinie](#)
- [Schritt 3: Eine Netzwerk-Firewall-Richtlinie erstellen und anwenden](#)

Schritt 1: Erfüllen Sie die allgemeinen Voraussetzungen

Mehrere Schritte sind zur Vorbereitung Ihres Kontos auf AWS Firewall Manager zwingend erforderlich. Diese Schritte werden in [AWS Firewall Manager Voraussetzungen](#) beschrieben. Erfüllen Sie alle Voraussetzungen, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 2: Erstellen Sie eine Netzwerk-Firewall-Regelgruppe zur Verwendung in Ihrer Richtlinie

Um diesem Tutorial zu folgen, sollten Sie mit den Regelgruppen AWS Network Firewall und Firewall-Richtlinien vertraut sein und wissen, wie man sie konfiguriert.

Sie müssen mindestens eine Regelgruppe in der Network Firewall haben, die in Ihrer AWS Firewall Manager Richtlinie verwendet wird. Wenn Sie noch keine Regelgruppe in der Network Firewall erstellt haben, tun Sie dies jetzt. Informationen zur Verwendung der Network Firewall finden Sie im [AWS Network Firewall Entwicklerhandbuch](#).

Schritt 3: Eine Netzwerk-Firewall-Richtlinie erstellen und anwenden

Nachdem Sie die Voraussetzungen erfüllt haben, erstellen Sie eine AWS Firewall Manager Netzwerk-Firewall-Richtlinie. Eine Netzwerk-Firewall-Richtlinie bietet eine zentral gesteuerte AWS Network Firewall für Ihr gesamtes AWS Unternehmen. Sie definiert auch die Ressourcen AWS-Konten und Ressourcen, für die die Firewall gilt.

Weitere Informationen darüber, wie Firewall Manager Ihre Netzwerk-Firewall-Richtlinien verwaltet, finden Sie unter [AWS Network Firewall Richtlinien](#).

So erstellen Sie eine Firewall Manager Manager-Netzwerk-Firewall-Richtlinie (Konsole)


1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).


2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wenn Sie die Voraussetzungen nicht erfüllt haben, zeigt die Konsole Anweisungen zur Behebung von Problemen an. Folgen Sie den Anweisungen und kehren Sie dann zu diesem Schritt zurück, um eine Netzwerk-Firewall-Richtlinie zu erstellen.
4. Wählen Sie Sicherheitsrichtlinie erstellen aus.

5. Wählen Sie unter Policy type (Richtlinientyp) die Option AWS Network Firewall.
6. Wählen Sie für Region eine aus AWS-Region.
7. Wählen Sie Weiter aus.
8. Geben Sie als Richtliniennamen einen aussagekräftigen Namen ein.
9. Die Richtlinienkonfiguration ermöglicht es Ihnen, die Firewall-Richtlinie zu definieren. Dies ist derselbe Prozess wie der, den Sie in der AWS Network Firewall Konsole verwenden. Sie fügen die Regelgruppen hinzu, die Sie in Ihrer Richtlinie verwenden möchten, und geben die standardmäßigen statusfreien Aktionen an. Für dieses Tutorial konfigurieren Sie diese Richtlinie wie eine Firewall-Richtlinie in Network Firewall.

 Note

Die automatische Korrektur erfolgt automatisch für AWS Firewall Manager Netzwerk-Firewall-Richtlinien, sodass Sie hier keine Option sehen, die auto Korrektur abzulehnen.

10. Wählen Sie Weiter aus.
11. Wählen Sie für Firewall-Endpunkte die Option Mehrere Firewall-Endpunkte aus. Diese Option bietet Hochverfügbarkeit für Ihre Firewall. Wenn Sie die Richtlinie erstellen, erstellt Firewall Manager in jeder Availability Zone, in der Sie öffentliche Subnetze schützen müssen, ein Firewall-Subnetz.
12. Wählen Sie für die AWS Network Firewall Routenkonfiguration die Option Überwachen, damit Firewall Manager Ihre VPCs auf Verstöße gegen die Routenkonfiguration überwacht und Sie mit Lösungsvorschlägen benachrichtigt, damit Sie die Richtlinien für die Routen einhalten können. Wenn Sie nicht möchten, dass Ihre Routenkonfigurationen von Firewall Manager überwacht werden und Sie diese Benachrichtigungen nicht erhalten, wählen Sie optional Aus.

 Note

Die Überwachung liefert Ihnen Details zu Ressourcen, die aufgrund einer fehlerhaften Routenkonfiguration nicht richtlinienkonform sind, und schlägt Korrekturmaßnahmen über die Firewall Manager `GetViolationDetails` Manager-API vor. Die Network Firewall warnt Sie beispielsweise, wenn der Datenverkehr nicht über die Firewall-Endpunkte geleitet wird, die durch Ihre Richtlinie erstellt wurden.

⚠ Warning

Wenn Sie Monitor wählen, können Sie es in future für dieselbe Richtlinie nicht mehr auf Aus ändern. Sie müssen eine neue Richtlinie erstellen.

13. Wählen Sie unter Verkehrstyp die Option Zur Firewall-Richtlinie hinzufügen aus, um den Datenverkehr über das Internet-Gateway weiterzuleiten.
14. AWS-Konten Mit der Option „Von dieser Richtlinie betroffen“ können Sie den Geltungsbereich Ihrer Richtlinie einschränken, indem Sie Konten angeben, die ein- oder ausgeschlossen werden sollen. In diesem Tutorial wählen Sie Include all accounts under my organization (Alle Konten in meiner Organisation einschließen).
15. Der Ressourcentyp für eine Netzwerk-Firewall-Richtlinie ist immer VPC.
16. Mit Resources (Ressourcen) können Sie den Geltungsbereich Ihrer Richtlinie einschränken, indem Sie Ressourcen-Tags für die Einbeziehung oder den Ausschluss angeben. Um Tagging zu verwenden, müssen Sie zuerst Ihre Ressourcen markieren. Weitere Informationen zum Kennzeichnen Ihrer Ressourcen finden Sie unter [Arbeiten mit Tag-Editor](#). Wählen Sie für dieses Tutorial Include all resources that match the selected resource type (Alle Ressourcen einschließen, die dem ausgewählten Ressourcentyp entsprechen).
17. Wählen Sie Weiter aus.
18. Überprüfen Sie Ihre Richtlinieneinstellungen und wählen Sie dann Richtlinie erstellen aus.

Im Bereich AWS Firewall Manager Richtlinien sollte Ihre Richtlinie aufgeführt sein. Die Erstellung einer Richtlinie kann mehrere Minuten dauern. Bis der Erstellungsprozess abgeschlossen ist, gibt die Richtlinie an, dass sie noch aussteht. Wenn die Richtlinie fertig ist, wird der Status mit der Anzahl der Konten im Geltungsbereich aktualisiert. Sie können den Namen der Richtlinie wählen, um den Konformitätsstatus der Konten und Ressourcen zu überprüfen. Weitere Informationen finden Sie unter [Compliance-Informationen für eine AWS Firewall Manager Richtlinie anzeigen](#)

19. Wenn Sie mit der Erkundung fertig sind und die Richtlinie, die Sie für dieses Tutorial erstellt haben, nicht behalten möchten, wählen Sie den Richtliniennamen aus, klicken Sie auf Löschen und dann auf Mit dieser Richtlinie erstellte Ressourcen bereinigen. , und wählen Sie schließlich Löschen.

Weitere Informationen zu den Netzwerk-Firewall-Richtlinien von Firewall Manager finden Sie unter [AWS Network Firewall Richtlinien](#).

Erste Schritte mit AWS Firewall Manager DNS-Firewall-Richtlinien

Um die Amazon Route 53 Resolver DNS Firewall in Ihrem Unternehmen zu aktivieren, führen Sie die folgenden Schritte nacheinander durch. AWS Firewall Manager Informationen zu den DNS-Firewallrichtlinien von Firewall Manager finden Sie unter [DNS-Firewall-Richtlinien für Amazon Route 53 Resolver](#).

Themen

- [Schritt 1: Erfüllen Sie die allgemeinen Voraussetzungen](#)
- [Schritt 2: Erstellen Sie Ihre DNS-Firewall-Regelgruppen zur Verwendung in Ihrer Richtlinie](#)
- [Schritt 3: Erstellen und Anwenden einer DNS-Firewall-Richtlinie](#)

Schritt 1: Erfüllen Sie die allgemeinen Voraussetzungen

Mehrere Schritte sind zur Vorbereitung Ihres Kontos auf AWS Firewall Manager zwingend erforderlich. Diese Schritte werden in [AWS Firewall Manager Voraussetzungen](#) beschrieben. Erfüllen Sie alle Voraussetzungen, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 2: Erstellen Sie Ihre DNS-Firewall-Regelgruppen zur Verwendung in Ihrer Richtlinie

Um diesem Tutorial zu folgen, sollten Sie mit der Amazon Route 53 Resolver DNS Firewall vertraut sein und wissen, wie die Regelgruppen konfiguriert werden.

Sie müssen mindestens eine Regelgruppe in der DNS-Firewall haben, die in Ihrer AWS Firewall Manager Richtlinie verwendet wird. Wenn Sie noch keine Regelgruppe in der DNS-Firewall erstellt haben, tun Sie dies jetzt. Informationen zur Verwendung der DNS-Firewall finden Sie unter [Amazon Route 53 Resolver DNS Firewall](#) im [Amazon Route 53 Developer Guide](#).

Schritt 3: Erstellen und Anwenden einer DNS-Firewall-Richtlinie

Nachdem Sie die Voraussetzungen erfüllt haben, erstellen Sie eine AWS Firewall Manager DNS-Firewall-Richtlinie. Eine DNS-Firewallrichtlinie bietet eine Reihe von zentral gesteuerten Zuordnungen von DNS-Firewall-Regelgruppen für Ihr gesamtes AWS Unternehmen. Sie definiert auch die Ressourcen AWS-Konten und Ressourcen, für die die Firewall gilt.

Weitere Informationen darüber, wie Firewall Manager Ihre DNS-Firewall-Regelgruppenzuordnungen verwaltet, finden Sie unter [DNS-Firewall-Richtlinien für Amazon Route 53 Resolver](#).

So erstellen Sie eine Firewall Manager Manager-DNS-Firewall-Richtlinie (Konsole)

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).
2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wenn Sie die Voraussetzungen nicht erfüllt haben, zeigt die Konsole Anweisungen zur Behebung von Problemen an. Folgen Sie den Anweisungen und kehren Sie dann zu diesem Schritt zurück, um eine DNS-Firewall-Richtlinie zu erstellen.
4. Wählen Sie Sicherheitsrichtlinie erstellen aus.
5. Wählen Sie als Richtlinientyp Amazon Route 53 Resolver DNS Firewall aus.
6. Wählen Sie für Region eine AWS-Region.
7. Wählen Sie Weiter aus.
8. Geben Sie als Richtliniennamen einen aussagekräftigen Namen ein.
9. Die Richtlinienkonfiguration ermöglicht es Ihnen, die Zuordnungen der DNS-Firewall-Regelgruppen zu definieren, die Sie über Firewall Manager verwalten möchten. Sie fügen die Regelgruppen hinzu, die Sie in Ihrer Richtlinie verwenden möchten. Sie können eine Zuordnung definieren, die zuerst für Ihre VPCs ausgewertet wird, und eine, die zuletzt ausgewertet wird. Fügen Sie für dieses Tutorial je nach Bedarf eine oder zwei Regelgruppenzuordnungen hinzu.
10. Wählen Sie Weiter aus.
11. AWS-Konten Mit der Option „von dieser Richtlinie betroffen“ können Sie den Geltungsbereich Ihrer Richtlinie einschränken, indem Sie Konten angeben, die ein- oder ausgeschlossen werden sollen. In diesem Tutorial wählen Sie Include all accounts under my organization (Alle Konten in meiner Organisation einschließen).
12. Der Ressourcentyp für eine DNS-Firewall-Richtlinie ist immer VPC.
13. Mit Resources (Ressourcen) können Sie den Geltungsbereich Ihrer Richtlinie einschränken, indem Sie Ressourcen-Tags für die Einbeziehung oder den Ausschluss angeben. Um Tagging zu verwenden, müssen Sie zuerst Ihre Ressourcen markieren. Weitere Informationen zum Kennzeichnen Ihrer Ressourcen finden Sie unter [Arbeiten mit Tag-Editor](#). Wählen Sie für dieses Tutorial Include all resources that match the selected resource type (Alle Ressourcen einschließen, die dem ausgewählten Ressourcentyp entsprechen).
14. Wählen Sie Weiter aus.
15. Überprüfen Sie Ihre Richtlinieneinstellungen und wählen Sie dann Richtlinie erstellen aus.

Im Bereich „AWS Firewall Manager Richtlinien“ sollte Ihre Richtlinie aufgeführt sein. Die Erstellung einer Richtlinie kann mehrere Minuten dauern. Bis der Erstellungsprozess abgeschlossen ist, gibt die Richtlinie an, dass sie noch aussteht. Wenn die Richtlinie fertig ist, wird der Status mit der Anzahl der Konten im Geltungsbereich aktualisiert. Sie können den Namen der Richtlinie wählen, um den Konformitätsstatus der Konten und Ressourcen zu überprüfen. Weitere Informationen finden Sie unter [Compliance-Informationen für eine AWS Firewall Manager Richtlinie anzeigen](#)

16. Wenn Sie mit der Erkundung fertig sind und die Richtlinie, die Sie für dieses Tutorial erstellt haben, nicht behalten möchten, wählen Sie den Richtliniennamen aus, klicken Sie auf Löschen und dann auf Mit dieser Richtlinie erstellte Ressourcen bereinigen. , und wählen Sie schließlich Löschen.

Weitere Informationen zu den DNS-Firewallrichtlinien von Firewall Manager finden Sie unter [DNS-Firewall-Richtlinien für Amazon Route 53 Resolver](#).

Erste Schritte mit den Cloud-Firewall-Richtlinien der nächsten Generation von AWS Firewall Manager Palo Alto Networks

Führen Sie die folgenden Schritte nacheinander aus, AWS Firewall Manager um die Cloud Next Generation Firewall (NGFW) -Richtlinien von Palo Alto Networks zu aktivieren. Informationen zu den Palo Alto Networks Cloud NGFW-Richtlinien finden Sie unter. [NGFW-Richtlinien für die Cloud von Palo Alto Networks](#)

Themen

- [Schritt 1: Erfüllen Sie die allgemeinen Voraussetzungen](#)
- [Schritt 2: Erfüllen Sie die Voraussetzungen für die Palo Alto Networks Cloud NGFW-Richtlinie](#)
- [Schritt 3: Eine Palo Alto Networks Cloud NGFW-Richtlinie erstellen und anwenden](#)

Schritt 1: Erfüllen Sie die allgemeinen Voraussetzungen

Mehrere Schritte sind zur Vorbereitung Ihres Kontos auf AWS Firewall Manager zwingend erforderlich. Diese Schritte werden in [AWS Firewall Manager Voraussetzungen](#) beschrieben. Erfüllen Sie alle Voraussetzungen, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 2: Erfüllen Sie die Voraussetzungen für die Palo Alto Networks Cloud NGFW-Richtlinie

Es gibt einige zusätzliche obligatorische Schritte, die Sie ausführen müssen, um die Palo Alto Networks Cloud NGFW-Richtlinien verwenden zu können. Diese Schritte werden in [Voraussetzungen für die Cloud-Firewall-Richtlinie der nächsten Generation von Palo Alto Networks](#) beschrieben.

Erfüllen Sie alle Voraussetzungen, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 3: Eine Palo Alto Networks Cloud NGFW-Richtlinie erstellen und anwenden

Nachdem Sie die Voraussetzungen erfüllt haben, erstellen Sie eine AWS Firewall Manager Palo Alto Networks Cloud NGFW-Richtlinie.

Weitere Informationen zu den Firewall Manager Manager-Richtlinien für Palo Alto Networks Cloud NGFW finden Sie unter [NGFW-Richtlinien für die Cloud von Palo Alto Networks](#)

So erstellen Sie eine Firewall Manager Manager-Richtlinie für Palo Alto Networks Cloud NGFW (Konsole)

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie als Richtlinientyp Palo Alto Networks Cloud NGFW aus. Wenn Sie den Palo Alto Networks Cloud NGFW-Dienst noch nicht im AWS Marketplace abonniert haben, müssen Sie dies zuerst tun. Um im AWS Marketplace ein Abonnement abzuschließen, wählen Sie AWS Marketplace-Details anzeigen.
5. Wählen Sie als Bereitstellungsmodell entweder das verteilte Modell oder das zentralisierte Modell. Das Bereitstellungsmodell bestimmt, wie Firewall Manager Endpunkte für die Richtlinie verwaltet. Beim verteilten Modell verwaltet Firewall Manager Firewall-Endpunkte in jeder VPC,

die innerhalb des Richtlinienbereichs liegen. Mit dem zentralisierten Modell verwaltet Firewall Manager einen einzigen Endpunkt in einer Inspektions-VPC.

6. Wählen Sie für Region eine AWS-Region. Um Ressourcen in mehreren Regionen zu schützen, müssen Sie für jede Region separate Richtlinien erstellen.
7. Wählen Sie Weiter aus.
8. Geben Sie als Richtlinienname einen aussagekräftigen Namen ein.
9. Wählen Sie in der Richtlinienkonfiguration die Palo Alto Networks Cloud NGFW-Firewallrichtlinie aus, die dieser Richtlinie zugeordnet werden soll. Die Liste der Palo Alto Networks Cloud NGFW-Firewallrichtlinien enthält alle Palo Alto Networks Cloud NGFW-Firewallrichtlinien, die Ihrem Palo Alto Networks Cloud NGFW-Mandanten zugeordnet sind. Informationen zum Erstellen und Verwalten von Palo Alto Networks Cloud NGFW-Firewallrichtlinien finden Sie im Abschnitt [Deploy Palo Alto Networks Cloud NGFW for](#) mit dem Thema im [Leitfaden Palo Alto Networks Cloud NGFW for Deployment](#). AWS AWS Firewall Manager AWS
10. Für die Palo Alto Networks Cloud NGFW-Protokollierung — optional — wählen Sie optional, welche Palo Alto Networks Cloud NGFW-Protokolltypen für Ihre Richtlinie protokolliert werden sollen. Informationen zu den NGFW-Protokolltypen in Palo Alto Networks Cloud finden [Sie unter Configure Logging for Palo Alto Networks Cloud NGFW on](#) im [Leitfaden Palo Alto Networks Cloud NGFW for Deployment](#). AWS AWS

Geben Sie als Protokollziel an, wohin Firewall Manager Protokolle schreiben soll.

11. Wählen Sie Weiter aus.
12. Führen Sie unter Firewall-Endpunkt eines Drittanbieters konfigurieren einen der folgenden Schritte aus, je nachdem, ob Sie für die Erstellung Ihrer Firewall-Endpunkte das verteilte oder das zentralisierte Bereitstellungsmodell verwenden:
 - Wenn Sie das verteilte Bereitstellungsmodell für diese Richtlinie verwenden, wählen Sie unter Availability Zones aus, in welchen Availability Zones Firewall-Endpoints erstellt werden sollen. Sie können Availability Zones nach dem Namen der Availability Zone oder nach der Availability Zone ID auswählen.
 - Wenn Sie das zentralisierte Bereitstellungsmodell für diese Richtlinie verwenden, geben Sie in der AWS Firewall Manager Endpunktkonfiguration unter Inspektion-VPC-Konfiguration die AWS Konto-ID des Besitzers der Inspektion-VPC und die VPC-ID der Inspektion-VPC ein.
 - Wählen Sie unter Availability Zones aus, in welchen Availability Zones Firewall-Endpoints erstellt werden sollen. Sie können Availability Zones nach dem Namen der Availability Zone oder nach der Availability Zone ID auswählen.

13. Wählen Sie Weiter aus.
14. Wählen Sie für den Geltungsbereich der Richtlinie unter „AWS-Konten Diese Richtlinie gilt für“ die Option wie folgt aus:
 - Wenn Sie die Richtlinie auf alle Konten in Ihrer Organisation anwenden möchten, behalten Sie die Standardauswahl Alle Konten meiner AWS Organisation einbeziehen bei.
 - Wenn Sie die Richtlinie nur auf bestimmte Konten oder Konten in bestimmten AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Nur die angegebenen Konten und Organisationseinheiten einbeziehen aus und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie einbeziehen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.
 - Wenn Sie die Richtlinie für alle Konten oder Organisationseinheiten (OUs) außer einer bestimmten Gruppe von Konten oder AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Die angegebenen Konten und Organisationseinheiten ausschließen und alle anderen einbeziehen aus, und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie ausschließen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

Sie können nur eine der Optionen auswählen.

Nachdem Sie die Richtlinie angewendet haben, bewertet Firewall Manager automatisch alle neuen Konten anhand Ihrer Einstellungen. Wenn Sie beispielsweise nur bestimmte Konten angeben, wendet Firewall Manager die Richtlinie nicht auf neue Konten an. Ein weiteres Beispiel: Wenn Sie eine Organisationseinheit hinzufügen und der Organisationseinheit oder einer ihrer untergeordneten Organisationseinheiten ein Konto hinzufügen, wendet Firewall Manager die Richtlinie automatisch auf das neue Konto an.

15. Der Ressourcentyp für Netzwerk-Firewall-Richtlinien ist VPC.
16. Wenn Sie unter Resources (Ressourcen) nur Ressourcen schützen (oder ausschließen) möchten, die bestimmte Tags haben, wählen Sie die entsprechende Option aus und geben Sie dann die Tags ein, die eingeschlossen oder ausgeschlossen werden sollen. Sie können nur eine Option auswählen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).

Wenn Sie mehrere Tags eingeben, muss eine Ressource über alle Tags verfügen, die eingeschlossen oder ausgeschlossen werden sollen.

17. Wählen Sie für Kontenübergreifenden Zugriff gewähren die Option Vorlage herunterladen AWS CloudFormation aus. Dadurch wird eine AWS CloudFormation Vorlage heruntergeladen, mit der Sie einen AWS CloudFormation Stack erstellen können. Dieser Stack erstellt eine AWS Identity and Access Management Rolle, die Firewall Manager kontoübergreifende Berechtigungen zur Verwaltung von Palo Alto Networks Cloud NGFW-Ressourcen gewährt. Informationen zu Stacks finden Sie unter [Arbeiten mit Stacks](#) im Benutzerhandbuch.AWS CloudFormation
18. Wählen Sie Weiter aus.
19. Fügen Sie für Policy-Tags alle Identifizierungs-Tags hinzu, die Sie für die Firewall Manager Manager-Richtlinie benötigen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).
20. Wählen Sie Weiter aus.
21. Überprüfen Sie die neue Richtlinie. Um Änderungen vorzunehmen, wählen Sie Edit (Bearbeiten) in dem Bereich, den Sie ändern möchten. Dadurch kehren Sie zum entsprechenden Schritt im Erstellungsassistenten zurück. Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen).

Weitere Informationen zu den Cloud NGFW-Richtlinien von Firewall Manager Palo Alto Networks finden Sie unter. [NGFW-Richtlinien für die Cloud von Palo Alto Networks](#)

Erste Schritte mit den AWS Firewall Manager Fortigate CNF-Richtlinien

Fortigate Cloud Native Firewall (CNF) as a Service ist ein Firewall-Service eines Drittanbieters, den Sie für Ihre Richtlinien verwenden können. AWS Firewall Manager Mit Fortigate CNF for Firewall Manager können Sie Fortigate CNF-Ressourcen und Richtlinienätze für all Ihre Konten erstellen und zentral bereitstellen. AWS Um Fortigate CNF-Richtlinien AWS Firewall Manager zu aktivieren, führen Sie die folgenden Schritte nacheinander aus. Weitere Informationen zu den Fortigate CNF-Richtlinien finden Sie unter. [Richtlinien für die Fortigate Cloud Native Firewall \(CNF\) als Service](#)

Themen

- [Schritt 1: Erfüllen Sie die allgemeinen Voraussetzungen](#)
- [Schritt 2: Erfüllen Sie die Voraussetzungen für die Fortigate CNF-Richtlinie](#)
- [Schritt 3: Eine Fortigate CNF-Richtlinie erstellen und anwenden](#)

Schritt 1: Erfüllen Sie die allgemeinen Voraussetzungen

Mehrere Schritte sind zur Vorbereitung Ihres Kontos auf AWS Firewall Manager zwingend erforderlich. Diese Schritte werden in [AWS Firewall Manager Voraussetzungen](#) beschrieben. Erfüllen Sie alle Voraussetzungen, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 2: Erfüllen Sie die Voraussetzungen für die Fortigate CNF-Richtlinie

Es gibt weitere obligatorische Schritte, die Sie ausführen müssen, um die Fortigate CNF-Richtlinien nutzen zu können. Diese Schritte werden in [Voraussetzungen für die Fortigate Cloud Native Firewall \(CNF\) as a Service-Richtlinie](#) beschrieben. Erfüllen Sie alle Voraussetzungen, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 3: Eine Fortigate CNF-Richtlinie erstellen und anwenden

Nachdem Sie die Voraussetzungen erfüllt haben, erstellen Sie eine AWS Firewall Manager Fortigate CNF-Richtlinie.

Weitere Informationen zu den Firewall Manager Manager-Richtlinien für Fortigate CNF finden Sie unter [Richtlinien für die Fortigate Cloud Native Firewall \(CNF\) als Service](#)

So erstellen Sie eine Firewall Manager Manager-Richtlinie für Fortigate CNF (Konsole)

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie als Richtlinientyp Fortigate CNF. Wenn Sie den Fortigate CNF-Service im AWS Marketplace noch nicht abonniert haben, müssen Sie dies zuerst tun. Um im AWS Marketplace ein Abonnement abzuschließen, wählen Sie AWS Marketplace-Details anzeigen.

5. Wählen Sie als Bereitstellungsmodell entweder das verteilte Modell oder das zentralisierte Modell. Das Bereitstellungsmodell bestimmt, wie Firewall Manager Endpunkte für die Richtlinie verwaltet. Beim verteilten Modell verwaltet Firewall Manager Firewall-Endpunkte in jeder VPC, die innerhalb des Richtlinienbereichs liegen. Mit dem zentralisierten Modell verwaltet Firewall Manager einen einzigen Endpunkt in einer Inspektions-VPC.
6. Wählen Sie für Region eine AWS-Region. Um Ressourcen in mehreren Regionen zu schützen, müssen Sie für jede Region separate Richtlinien erstellen.
7. Wählen Sie Weiter aus.
- 8.
9. Wählen Sie in der Richtlinienkonfiguration die Fortigate CNF-Firewall-Richtlinie aus, die dieser Richtlinie zugeordnet werden soll. Die Liste der Fortigate CNF-Firewallrichtlinien enthält alle Fortigate CNF-Firewallrichtlinien, die Ihrem Fortigate CNF-Mandanten zugeordnet sind. [Informationen zur Erstellung und Verwaltung von Fortigate CNF-Firewallrichtlinien finden Sie in der Fortigate CNF-Dokumentation.](#)
10. Wählen Sie Weiter aus.
11. Führen Sie unter Firewall-Endpunkt eines Drittanbieters konfigurieren einen der folgenden Schritte aus, je nachdem, ob Sie für die Erstellung Ihrer Firewall-Endpunkte das verteilte oder das zentralisierte Bereitstellungsmodell verwenden:
 - Wenn Sie das verteilte Bereitstellungsmodell für diese Richtlinie verwenden, wählen Sie unter Availability Zones aus, in welchen Availability Zones Firewall-Endpoints erstellt werden sollen. Sie können Availability Zones nach dem Namen der Availability Zone oder nach der Availability Zone ID auswählen.
 - Wenn Sie das zentralisierte Bereitstellungsmodell für diese Richtlinie verwenden, geben Sie in der AWS Firewall Manager Endpunktkonfiguration unter Inspektion-VPC-Konfiguration die AWS Konto-ID des Besitzers der Inspektion-VPC und die VPC-ID der Inspektion-VPC ein.
 - Wählen Sie unter Availability Zones aus, in welchen Availability Zones Firewall-Endpoints erstellt werden sollen. Sie können Availability Zones nach dem Namen der Availability Zone oder nach der Availability Zone ID auswählen.
12. Wählen Sie Weiter aus.
13. Wählen Sie für den Geltungsbereich der Richtlinie unter „AWS-Konten Diese Richtlinie gilt für“ die Option wie folgt aus:
 - Wenn Sie die Richtlinie auf alle Konten in Ihrer Organisation anwenden möchten, behalten Sie die Standardauswahl Alle Konten meiner AWS Organisation einbeziehen bei.

- Wenn Sie die Richtlinie nur auf bestimmte Konten oder Konten in bestimmten AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Nur die angegebenen Konten und Organisationseinheiten einbeziehen aus und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie einbeziehen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.
- Wenn Sie die Richtlinie für alle Konten oder Organisationseinheiten (OUs) außer einer bestimmten Gruppe von Konten oder AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Die angegebenen Konten und Organisationseinheiten ausschließen und alle anderen einbeziehen aus, und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie ausschließen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

Sie können nur eine der Optionen auswählen.

Nachdem Sie die Richtlinie angewendet haben, bewertet Firewall Manager automatisch alle neuen Konten anhand Ihrer Einstellungen. Wenn Sie beispielsweise nur bestimmte Konten angeben, wendet Firewall Manager die Richtlinie nicht auf neue Konten an. Ein weiteres Beispiel: Wenn Sie eine Organisationseinheit hinzufügen und der Organisationseinheit oder einer ihrer untergeordneten Organisationseinheiten ein Konto hinzufügen, wendet Firewall Manager die Richtlinie automatisch auf das neue Konto an.

14. Der Ressourcentyp für Netzwerk-Firewall-Richtlinien ist VPC.
15. Wenn Sie unter Resources (Ressourcen) nur Ressourcen schützen (oder ausschließen) möchten, die bestimmte Tags haben, wählen Sie die entsprechende Option aus und geben Sie dann die Tags ein, die eingeschlossen oder ausgeschlossen werden sollen. Sie können nur eine Option auswählen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).

Wenn Sie mehrere Tags eingeben, muss eine Ressource über alle Tags verfügen, die eingeschlossen oder ausgeschlossen werden sollen.

16. Wählen Sie für Kontenübergreifenden Zugriff gewähren die Option Vorlage herunterladen AWS CloudFormation aus. Dadurch wird eine AWS CloudFormation Vorlage heruntergeladen, mit der Sie einen AWS CloudFormation Stack erstellen können. Dieser Stack erstellt eine AWS Identity and Access Management Rolle, die Firewall Manager kontoübergreifende Berechtigungen zur

Verwaltung von Fortigate CNF-Ressourcen gewährt. Informationen zu Stacks finden Sie unter [Arbeiten mit Stacks](#) im Benutzerhandbuch.AWS CloudFormation Um einen Stack zu erstellen, benötigen Sie die Konto-ID aus dem Fortigate CNF-Portal.

17. Wählen Sie Weiter aus.
18. Fügen Sie für Policy-Tags alle Identifizierungs-Tags hinzu, die Sie für die Firewall Manager Manager-Richtlinie benötigen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).
19. Wählen Sie Weiter aus.
20. Überprüfen Sie die neue Richtlinie. Um Änderungen vorzunehmen, wählen Sie Edit (Bearbeiten) in dem Bereich, den Sie ändern möchten. Dadurch kehren Sie zum entsprechenden Schritt im Erstellungsassistenten zurück. Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen).

Weitere Informationen zu den CNF-Richtlinien von Firewall Manager Fortigate finden Sie unter [Richtlinien für die Fortigate Cloud Native Firewall \(CNF\) als Service](#)

Mit AWS Firewall Manager Richtlinien arbeiten

AWS Firewall Manager bietet die folgenden Arten von Richtlinien:

- **AWS WAF Richtlinie** — Firewall Manager unterstützt AWS WAF AWS WAF klassische Richtlinien. Für beide Versionen legen Sie fest, welche Ressourcen durch die Richtlinie geschützt sind.
 - Für die AWS WAF Richtlinie können Sie eine Reihe von Regelgruppen definieren, die zuerst in der Web-ACL ausgeführt werden, und eine Reihe von Regelgruppen, die zuletzt ausgeführt werden. In den Konten, für die Sie die Web-ACL anwenden, kann der Kontoinhaber Regeln und Regelgruppen hinzufügen, die zwischen den beiden Firewall Manager Manager-Regelgruppensätzen ausgeführt werden.
 - Für AWS WAF Classic erstellen Sie eine Richtlinie, die eine einzelne Regelgruppe definiert.
- **Shield Advanced-Richtlinie** — Diese Richtlinie wendet AWS Shield Advanced Schutz auf bestimmte Konten und Ressourcen an.
- **Amazon VPC-Sicherheitsgruppenrichtlinie** — Diese Art von Richtlinie gibt Ihnen die Kontrolle über Sicherheitsgruppen, die in Ihrer gesamten Organisation verwendet werden, AWS Organizations und ermöglicht es Ihnen, grundlegende Regeln in Ihrer gesamten Organisation durchzusetzen.
- **Netzwerk-Firewall-Richtlinie** — Diese Richtlinie AWS Network Firewall schützt die VPCs Ihres Unternehmens.

- **Amazon Route 53 Resolver DNS-Firewall-Richtlinie** — Diese Richtlinie wendet DNS-Firewall-Schutz auf die VPCs Ihres Unternehmens an.
- **Firewall-Richtlinie von Drittanbietern** — Diese Richtlinie wendet Firewall-Schutzmaßnahmen von Drittanbietern an. Firewalls von Drittanbietern sind als Abonnement über die AWS Marketplace-Konsole auf [AWS Marketplace](#) erhältlich.
 - **Palo Alto Networks Cloud NGFW-Richtlinie** — Diese Richtlinie wendet die Palo Alto Networks Cloud Next Generation Firewall (NGFW) -Schutzmaßnahmen und die Palo Alto Networks Cloud NGFW-Regeln auf die VPCs Ihres Unternehmens an.
 - **Richtlinie für Fortigate Cloud Native Firewall (CNF) as a Service** — Diese Richtlinie wendet die Schutzmaßnahmen der Fortigate Cloud Native Firewall (CNF) as a Service an. Fortigate CNF ist eine Cloud-zentrierte Lösung, die Zero-Day-Bedrohungen blockiert und Cloud-Infrastrukturen mit branchenführender fortschrittlicher Bedrohungsabwehr, intelligenten Web Application Firewalls (WAF) und API-Schutz schützt.

Eine Firewall Manager Richtlinie ist spezifisch für den einzelnen Richtlinientyp. Wenn Sie mehrere Richtlinientypen kontenübergreifend durchsetzen möchten, können Sie mehrere Richtlinien erstellen. Sie können mehr als eine Richtlinie für jeden Typ erstellen.

Wenn Sie einer Organisation AWS Organizations, mit der Sie das Konto erstellt haben, ein neues Konto hinzufügen, wendet Firewall Manager die Richtlinie automatisch auf die Ressourcen in diesem Konto an, die in den Geltungsbereich der Richtlinie fallen.

Allgemeine Einstellungen für AWS Firewall Manager Richtlinien

AWS Firewall Manager verwaltete Richtlinien haben einige allgemeine Einstellungen und Verhaltensweisen. Für alle geben Sie einen Namen an und definieren den Geltungsbereich der Richtlinie, und Sie können den Geltungsbereich der Richtlinie mithilfe von Ressourcen-Tagging steuern. Sie können die Konten und Ressourcen anzeigen, die nicht konform sind, ohne Korrekturmaßnahmen zu ergreifen oder nicht konforme Ressourcen automatisch zu korrigieren.

Informationen zum Geltungsbereich der Richtlinie finden Sie unter [AWS Firewall Manager Geltungsbereich der Politik](#).

Eine AWS Firewall Manager Richtlinie erstellen

Die Schritte zum Erstellen einer Richtlinie variieren zwischen den verschiedenen Richtlinientypen. Stellen Sie sicher, dass Sie das Verfahren für den gewünschten Richtlinientyp verwenden.

⚠ Important

AWS Firewall Manager unterstützt Amazon Route 53 nicht oder AWS Global Accelerator. Wenn Sie diese Ressourcen mit Shield Advanced schützen möchten, können Sie keine Firewall Manager Manager-Richtlinie verwenden. Folgen Sie stattdessen den Anweisungen in [AWS Shield Advanced Schutz für Ressourcen hinzufügen AWS](#).

Themen

- [Eine AWS Firewall Manager Richtlinie erstellen für AWS WAF](#)
- [Eine AWS Firewall Manager Richtlinie für AWS WAF Classic erstellen](#)
- [Eine AWS Firewall Manager Richtlinie erstellen für AWS Shield Advanced](#)
- [Erstellen einer gemeinsamen AWS Firewall Manager -Sicherheitsgruppenrichtlinie](#)
- [Erstellen einer AWS Firewall Manager -Inhaltsprüfungssicherheitsgruppenrichtlinie](#)
- [Erstellen einer AWS Firewall Manager -Nutzungsprüfungssicherheitsgruppenrichtlinie](#)
- [Eine AWS Firewall Manager Richtlinie erstellen für AWS Network Firewall](#)
- [Erstellen einer AWS Firewall Manager Richtlinie für Amazon Route 53 Resolver DNS Firewall](#)
- [Eine AWS Firewall Manager Richtlinie für Palo Alto Networks Cloud NGFW erstellen](#)
- [Erstellen einer AWS Firewall Manager Richtlinie für Fortigate Cloud Native Firewall \(CNF\) as a Service](#)

Eine AWS Firewall Manager Richtlinie erstellen für AWS WAF

In einer Firewall Manager AWS WAF Manager-Richtlinie können Sie verwaltete Regelgruppen verwenden, die AWS von AWS Marketplace Verkäufern für Sie erstellt und verwaltet werden. Sie können auch eigene Regelgruppen erstellen und verwenden. Weitere Informationen zu Regelgruppen finden Sie unter [Regelgruppen](#).

Wenn Sie Ihre eigenen Regelgruppen verwenden möchten, erstellen Sie diese, bevor Sie Ihre Firewall Manager AWS WAF Manager-Richtlinie erstellen. Anleitungen finden Sie unter [Verwaltung Ihrer eigenen Regelgruppen](#). Um eine einzelne benutzerdefinierte Regel verwenden zu können, müssen Sie eine eigene Regelgruppe definieren, Ihre Regel darin definieren und dann die Regelgruppe in der Richtlinie verwenden.

Informationen zu den AWS WAF Richtlinien von Firewall Manager finden Sie unter [AWS WAF Richtlinien](#).

So erstellen Sie eine Firewall Manager Manager-Richtlinie für AWS WAF (Konsole)

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie unter Policy type (Richtlinientyp) die Option AWS WAF.
5. Wählen Sie für Region eine AWS-Region. Um CloudFront Amazon-Distributionen zu schützen, wählen Sie Global.

Um Ressourcen in mehreren Regionen (außer CloudFront Verteilungen) zu schützen, müssen Sie separate Firewall Manager Manager-Richtlinien für jede Region erstellen.

6. Wählen Sie Weiter aus.
7. Geben Sie als Richtliniename einen aussagekräftigen Namen ein. Firewall Manager nimmt den Richtliniennamen in die Namen der Web-ACLs auf, die er verwaltet. Auf die Web-ACL-Namen FMMangedWebACLV2- folgten der Richtliniename, den Sie hier eingeben-, und der Zeitstempel für die Erstellung der Web-ACL in UTC-Millisekunden. z. B. FMMangedWebACLV2-MyWAFPolicyName-1621880374078.
8. Bei der Körperinspektion von Webanfragen können Sie optional die Körpergrößenbeschränkung ändern. Informationen zu Größenbeschränkungen bei Karosserieinspektionen, einschließlich Preisüberlegungen, finden Sie [Verwaltung der Größenbeschränkungen bei Körperinspektionen](#) im AWS WAF Entwicklerhandbuch.
9. Fügen Sie unter Richtlinienregeln die Regelgruppen, die Sie zuerst und zuletzt auswerten AWS WAF möchten, in der Web-ACL hinzu. Um die AWS WAF verwaltete Regelgruppen-Versionsverwaltung zu verwenden, aktivieren Sie die Option Versionierung aktivieren. Die einzelnen Kontomanager können zwischen den ersten Regelgruppen und den letzten Regelgruppen Regeln und Regelgruppen hinzufügen. Weitere Informationen zur Verwendung

von AWS WAF Regelgruppen in Firewall Manager Manager-Richtlinien für AWS WAF finden Sie unter [AWS WAF Richtlinien](#).

(Optional) Um anzupassen, wie Ihre Web-ACL die Regelgruppe verwendet, wählen Sie Bearbeiten. Im Folgenden finden Sie allgemeine Anpassungseinstellungen:

- Überschreiben Sie bei verwalteten Regelgruppen die Regelaktionen für einige oder alle Regeln. Wenn Sie keine Aktion zum Außerkraftsetzen für eine Regel definieren, verwendet die Auswertung die Regelaktion, die innerhalb der Regelgruppe definiert ist. Informationen zu dieser Option finden Sie [Aktionsüberschreibungen in Regelgruppen](#) im AWS WAF Entwicklerhandbuch.
- Bei einigen verwalteten Regelgruppen müssen Sie zusätzliche Konfigurationen angeben. Weitere Informationen finden Sie in der Dokumentation Ihres Anbieters für verwaltete Regelgruppen. Spezifische Informationen zu den Regelgruppen für AWS verwaltete Regeln finden Sie [AWS Verwaltete Regeln für AWS WAF](#) im AWS WAF Entwicklerhandbuch.

Wenn Sie mit Ihren Einstellungen fertig sind, wählen Sie Regel speichern.

10. Stellen Sie die Standardaktion für die Web-ACL ein. Dies ist die Aktion, die AWS WAF ergreift, wenn eine Webanforderung keiner der Regeln in der Web-ACL entspricht. Sie können benutzerdefinierte Header mit der Aktion Zulassen oder benutzerdefinierte Antworten mit der Aktion Blockieren hinzufügen. Weitere Informationen zu standardmäßigen Web-ACL-Aktionen finden Sie unter [Die Web-ACL-Standardaktion](#). Informationen zum Einrichten benutzerdefinierter Webanfragen und -antworten finden Sie unter [Benutzerdefinierte Webanforderungen und Antworten in AWS WAF](#).
11. Wählen Sie für die Konfiguration der Protokollierung die Option Protokollierung aktivieren aus, um die Protokollierung zu aktivieren. Die Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. Wählen Sie das Protokollierungsziel und dann das von Ihnen konfigurierte Protokollierungsziel aus. Sie müssen ein Protokollierungsziel auswählen, dessen Name mit `aws-waf-logs-` beginnt. Informationen zur Konfiguration eines AWS WAF Protokollierungsziels finden Sie unter [Konfiguration der Protokollierung für eine Richtlinie AWS WAF](#).
12. (Optional) Wenn Sie nicht möchten, dass bestimmte Felder und deren Werte in den Protokollen enthalten sind, machen Sie diese Felder unkenntlich. Wählen Sie das Feld aus, das unkenntlich gemacht werden soll, und klicken Sie dann auf Add (Hinzufügen). Wiederholen Sie diesen Vorgang nach Bedarf, um zusätzliche Felder unkenntlich zu machen. Die unkenntlich gemachten

Felder werden als REDACTED in den Protokollen angezeigt. Wenn Sie beispielsweise das Feld URI unkenntlich machen, wird das Feld URI in den Protokollen als REDACTED angezeigt.

13. (Optional) Wenn Sie nicht alle Anforderungen an die Protokolle senden möchten, fügen Sie Filterkriterien und -verhalten hinzu. Wählen Sie unter Filter logs (Protokolle filtern) für jeden Filter, den Sie anwenden möchten, Add filter (Filter hinzufügen) aus. Wählen Sie dann Ihre Filterkriterien und geben Sie an, ob Sie Anforderungen, die den Kriterien entsprechen, beibehalten oder löschen möchten. Wenn Sie mit dem Hinzufügen von Filtern fertig sind, ändern Sie bei Bedarf das Standardprotokollierungsverhalten. Weitere Informationen finden Sie unter [Verwalten der Protokollierung für eine Web-ACL](#) im AWS WAF -Entwicklerhandbuch.
14. Sie können eine Token-Domainliste definieren, um die gemeinsame Nutzung von Token zwischen geschützten Anwendungen zu ermöglichen. Tokens werden von den Challenge Aktionen CAPTCHA und von den Anwendungsintegrations-SDKs verwendet, die Sie implementieren, wenn Sie die Regelgruppen AWS Managed Rules für Accountübernahmeprevention (ATP) und AWS WAF Bot-Kontrolle bei der AWS WAF Betrugsbekämpfung verwenden.

Öffentliche Suffixe sind nicht zulässig. Beispielsweise können Sie gov . au oder nicht co . uk als Token-Domain verwenden.

AWS WAF Akzeptiert standardmäßig nur Token für die Domäne der geschützten Ressource. Wenn Sie Tokendomänen zu dieser Liste hinzufügen, AWS WAF akzeptiert Tokens für alle Domänen in der Liste und für die Domäne der zugehörigen Ressource. Weitere Informationen finden Sie unter [Konfiguration der Domainliste für Web-ACL-Tokens](#) im AWS WAF -Entwicklerhandbuch.

Sie können die CAPTCHA- und Challenge-Immunitätszeiten der Web-ACL nur ändern, wenn Sie eine bestehende Web-ACL bearbeiten. Sie finden diese Einstellungen auf der Seite mit den Details zur Firewall Manager Manager-Richtlinie. Weitere Informationen zu diesen Einstellungen finden Sie unter [Ablauf des Zeitstempels: Zeiten der Token-Immunität](#). Wenn Sie die Einstellungen für die Zuordnungskonfiguration, CAPTCHA, Challenge oder Token-Domainliste in einer vorhandenen Richtlinie aktualisieren, überschreibt Firewall Manager Ihre lokalen Web-ACLs mit den neuen Werten. Wenn Sie jedoch die Einstellungen für die Zuordnungskonfiguration, CAPTCHA, Challenge oder Token-Domänenliste der Richtlinie nicht aktualisieren, bleiben die Werte in Ihren lokalen Web-ACLs unverändert. Informationen zu dieser Option finden Sie [CAPTCHA und Challenge in AWS WAF](#) im Entwicklerhandbuch.

15. Wenn Sie möchten, dass Firewall Manager nicht verknüpfte Web-ACLs verwaltet, aktivieren Sie unter Web-ACLs verwalten die Option Nicht verknüpfte Web-ACLs verwalten. Mit dieser

Option erstellt Firewall Manager Web-ACLs in den Konten innerhalb des Richtlinienbereichs nur dann, wenn die Web-ACLs von mindestens einer Ressource verwendet werden. Wenn ein Konto zu irgendeinem Zeitpunkt in den Geltungsbereich der Richtlinie fällt, erstellt Firewall Manager automatisch eine Web-ACL in dem Konto, sofern mindestens eine Ressource die Web-ACL verwendet. Nach der Aktivierung dieser Option führt Firewall Manager eine einmalige Bereinigung der nicht verknüpften Web-ACLs in Ihrem Konto durch. Der Bereinigungsprozess kann mehrere Stunden dauern. Wenn eine Ressource den Richtlinienbereich verlässt, nachdem Firewall Manager eine Web-ACL erstellt hat, trennt Firewall Manager die Zuordnung der Ressource von der Web-ACL, bereinigt aber nicht die nicht zugeordnete Web-ACL. Firewall Manager bereinigt nicht verknüpfte Web-ACLs nur, wenn Sie die Verwaltung nicht verknüpfter Web-ACLs in einer Richtlinie zum ersten Mal aktivieren.

16. Wenn Sie für Richtlinienaktion eine Web-ACL für jedes entsprechende Konto innerhalb der Organisation erstellen, die Web-ACL aber noch nicht auf Ressourcen anwenden möchten, wählen Sie Ressourcen identifizieren, die nicht den Richtlinienregeln entsprechen, aber keine auto Korrektur durchführen und wählen Sie nicht zugeordnete Web-ACLs verwalten aus. Sie können diese Optionen später ändern.

Wenn Sie die Richtlinie stattdessen automatisch auf vorhandene Ressourcen im Bereich anwenden möchten, wählen Sie Auto remediate any noncompliant resources (Alle nicht konformen Ressourcen automatisch korrigieren) aus. Wenn „Nicht verknüpfte Web-ACLs verwalten“ deaktiviert ist, erstellt die Option Nicht konforme Ressourcen automatisch korrigieren für jedes entsprechende Konto innerhalb der Organisation eine Web-ACL und ordnet die Web-ACL den Ressourcen in den Konten zu. Wenn die Option Nicht verknüpfte Web-ACLs verwalten aktiviert ist, erstellt und ordnet die Option Nicht konforme Ressourcen automatisch korrigieren nur Konten, deren Ressourcen für die Zuordnung zur Web-ACL in Frage kommen, eine Web-ACL zu.

Wenn Sie die Option Nicht konforme Ressourcen automatisch korrigieren wählen, können Sie auch festlegen, dass bestehende Web-ACL-Zuordnungen aus Ressourcen im Geltungsbereich entfernt werden, und zwar für Web-ACLs, die nicht durch eine andere aktive Firewall Manager Richtlinie verwaltet werden. Wenn Sie diese Option wählen, ordnet Firewall Manager zuerst die Web-ACL der Richtlinie den Ressourcen zu und entfernt dann die vorherigen Zuordnungen. Wenn eine Ressource mit einer anderen Web-ACL verknüpft ist, die von einer anderen aktiven Firewall Manager Richtlinie verwaltet wird, wirkt sich diese Auswahl nicht auf diese Zuordnung aus.

17. Wählen Sie Weiter aus.
18. Wenn AWS-Konten diese Richtlinie für gilt, wählen Sie die Option wie folgt aus:

- Wenn Sie die Richtlinie auf alle Konten in Ihrer Organisation anwenden möchten, behalten Sie die Standardauswahl Alle Konten meiner AWS Organisation einbeziehen bei.
- Wenn Sie die Richtlinie nur auf bestimmte Konten oder Konten in bestimmten AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Nur die angegebenen Konten und Organisationseinheiten einbeziehen aus und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie einbeziehen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.
- Wenn Sie die Richtlinie auf alle Konten und Organisationseinheiten mit Ausnahme einer bestimmten Gruppe von Konten oder AWS Organizations -Organisationseinheiten (OUs) anwenden möchten, wählen Sie Exclude the specified accounts and organizational units, and include all others (Die angegebenen Konten und Organisationseinheiten ausschließen und alle anderen einschließen) aus und fügen Sie dann die Konten und OUs hinzu, die Sie ausschließen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

Sie können nur eine der Optionen auswählen.

Nachdem Sie die Richtlinie angewendet haben, bewertet Firewall Manager automatisch alle neuen Konten anhand Ihrer Einstellungen. Wenn Sie beispielsweise nur bestimmte Konten angeben, wendet Firewall Manager die Richtlinie nicht auf neue Konten an. Ein weiteres Beispiel: Wenn Sie eine Organisationseinheit hinzufügen und der Organisationseinheit oder einer ihrer untergeordneten Organisationseinheiten ein Konto hinzufügen, wendet Firewall Manager die Richtlinie automatisch auf das neue Konto an.

19. Wählen Sie unter Resource type (Ressourcentyp) die Arten von Ressourcen aus, die Sie schützen möchten.
20. Wenn Sie unter Resources (Ressourcen) nur Ressourcen schützen (oder ausschließen) möchten, die bestimmte Tags haben, wählen Sie die entsprechende Option aus und geben Sie dann die Tags ein, die eingeschlossen oder ausgeschlossen werden sollen. Sie können nur eine Option auswählen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).

Wenn Sie mehrere Tags eingeben, muss eine Ressource über alle Tags verfügen, die eingeschlossen oder ausgeschlossen werden sollen.

21. Wählen Sie Weiter aus.
22. Fügen Sie für Policy-Tags alle Identifizierungs-Tags hinzu, die Sie für die Firewall Manager Manager-Richtlinie benötigen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).
23. Wählen Sie Weiter aus.
24. Überprüfen Sie die neue Richtlinie. Um Änderungen vorzunehmen, wählen Sie Edit (Bearbeiten) in dem Bereich, den Sie ändern möchten. Dadurch kehren Sie zum entsprechenden Schritt im Erstellungsassistenten zurück. Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen).

Eine AWS Firewall Manager Richtlinie für AWS WAF Classic erstellen

So erstellen Sie eine Firewall Manager Manager-Richtlinie für AWS WAF Classic (Konsole)

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie unter Policy type (Richtlinientyp) die Option AWS WAF Classic aus.
5. Wenn Sie die AWS WAF klassische Regelgruppe, die Sie der Richtlinie hinzufügen möchten, bereits erstellt haben, wählen Sie AWS Firewall Manager Richtlinie erstellen und vorhandene Regelgruppen hinzufügen aus. Wenn Sie eine neue Regelgruppe erstellen möchten, wählen Sie Create a Firewall Manager Policy und fügen Sie eine neue Regelgruppe hinzu.
6. Wählen Sie für Region eine AWS-Region. Um CloudFront Amazon-Ressourcen zu schützen, wählen Sie Global.

Um Ressourcen in mehreren Regionen (außer CloudFront Ressourcen) zu schützen, müssen Sie separate Firewall Manager Manager-Richtlinien für jede Region erstellen.

7. Wählen Sie Weiter aus.
8. Wenn Sie eine Regelgruppe erstellen, befolgen Sie die Anweisungen unter [Eine AWS WAF klassische Regelgruppe erstellen](#). Fahren Sie nach dem Erstellen der Regelgruppe mit den folgenden Schritten fort.
9. Geben Sie den Namen einer Richtlinie ein.
10. Wenn Sie eine vorhandene Regelgruppe hinzufügen, wählen Sie im Dropdownmenü die entsprechende Regelgruppe aus und wählen Sie dann die Option Add rule group (Regelgruppe hinzufügen).
11. Für eine Richtlinie sind zwei mögliche Aktionen vorhanden: Action set by rule group (Aktion durch Regelgruppe festgelegt) und Count (Zählen). Wenn Sie die Richtlinie und Regelgruppe testen möchten, legen Sie als Aktion Count (Zählen) fest. Diese Aktion setzt jede durch die Regeln in der Regelgruppe festgelegte Aktion zum Blockieren außer Kraft. Wenn als Aktion der Richtlinie Count (Zählen) festgelegt ist, bedeutet dies, dass solche Anforderungen nur gezählt und nicht blockiert werden. Wenn Sie als Aktion der Richtlinie dagegen Action set by rule group (Aktion durch Regelgruppe festgelegt) festlegen, werden Aktionen der Regelgruppenregeln verwendet. Wählen Sie die geeignete Aktion aus.
12. Wählen Sie Weiter aus.
13. Wenn AWS-Konten diese Richtlinie gilt für, wählen Sie die Option wie folgt aus:
 - Wenn Sie die Richtlinie auf alle Konten in Ihrer Organisation anwenden möchten, behalten Sie die Standardauswahl Alle Konten meiner AWS Organisation einbeziehen bei.
 - Wenn Sie die Richtlinie nur auf bestimmte Konten oder Konten in bestimmten AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Nur die angegebenen Konten und Organisationseinheiten einbeziehen aus und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie einbeziehen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.
 - Wenn Sie die Richtlinie für alle Konten oder Organisationseinheiten (OUs) außer einer bestimmten Gruppe von Konten oder AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Die angegebenen Konten und Organisationseinheiten ausschließen und alle anderen einbeziehen aus, und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie ausschließen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs,

einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

Sie können nur eine der Optionen auswählen.

Nachdem Sie die Richtlinie angewendet haben, bewertet Firewall Manager automatisch alle neuen Konten anhand Ihrer Einstellungen. Wenn Sie beispielsweise nur bestimmte Konten angeben, wendet Firewall Manager die Richtlinie nicht auf neue Konten an. Ein weiteres Beispiel: Wenn Sie eine Organisationseinheit hinzufügen und der Organisationseinheit oder einer ihrer untergeordneten Organisationseinheiten ein Konto hinzufügen, wendet Firewall Manager die Richtlinie automatisch auf das neue Konto an.

14. Wählen Sie den Ressourcentyp aus, der geschützt werden soll.
15. Wenn Sie nur Ressourcen mit bestimmten Tags schützen oder alternativ Ressourcen mit bestimmten Tags ausschließen möchten, wählen Sie Use tags to include/exclude resources (Ressourcen mittels Tags ein-/ausschließen), geben Sie die Tags ein, und wählen Sie entweder Include (Einschließen) oder Exclude (Ausschließen). Sie können nur eine Option auswählen.

Wenn Sie mehr als einen Tag (durch Kommas getrennt) eingeben, gelten alle Ressourcen mit einem dieser Tags als Entsprechung.

Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).

16. Wenn die Richtlinie automatisch auf vorhandene Richtlinien angewendet werden soll, wählen Sie Create and apply this policy to existing and new resources (Diese Richtlinie erstellen und auf vorhandene und neue Ressourcen anwenden).

Diese Option erstellt eine Web-ACL für alle entsprechenden Konten innerhalb einer AWS - Organisation und ordnet die Web-ACL den angegebenen Ressourcen in den Konten zu. Diese Option wendet die Richtlinie auch auf alle neuen Ressourcen an, die den voranstehenden Kriterien (Ressourcentyp und Tags) entsprechen. Alternativ erstellt Firewall Manager bei Wahl von Create policy but do not apply the policy to existing or new resources (Richtlinie erstellen, aber nicht auf vorhandene oder neue Ressourcen anwenden) in jedem entsprechenden Konto innerhalb der Organisation eine Web-ACL, wendet die Web-ACL jedoch nicht auf Ressourcen an. Sie müssen die Richtlinie zu einem späteren Zeitpunkt auf Ressourcen anwenden. Wählen Sie die geeignete Option aus.

17. Für Replace existing associated web ACLs (Vorhandene zugeordnete Web-ACLs ersetzen) können Sie festlegen, dass alle Web-ACL-Zuordnungen entfernt werden, die derzeit für Ressourcen im Bereich definiert sind, und diese dann durch Zuordnungen zu den Web-ACLs

ersetzt werden, die Sie mit dieser Richtlinie erstellen. Standardmäßig entfernt Firewall Manager vorhandene Web-ACL-Zuordnungen nicht, bevor die neuen hinzugefügt werden. Wenn Sie die vorhandenen Zuordnungen entfernen möchten, wählen Sie diese Option aus.

18. Wählen Sie Weiter aus.
19. Überprüfen Sie die neue Richtlinie. Um Änderungen vorzunehmen, wählen Sie Edit (Bearbeiten). Wenn Sie mit der Richtlinie zufrieden sind, wählen Sie Create and apply Policy (Richtlinie erstellen und anwenden).

Eine AWS Firewall Manager Richtlinie erstellen für AWS Shield Advanced

So erstellen Sie eine Firewall Manager Manager-Richtlinie für Shield Advanced (Konsole)

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie als Richtlinientyp Shield Advanced aus.

Um eine Shield Advanced-Richtlinie zu erstellen, müssen Sie Shield Advanced abonniert haben. Wenn Sie kein Abonnement eingerichtet haben, werden Sie dazu aufgefordert. [Informationen zu den Kosten für ein Abonnement finden Sie unter AWS Shield Advanced Preise](#).

5. Wählen Sie für Region eine AWS-Region. Um CloudFront Amazon-Distributionen zu schützen, wählen Sie Global.

Für andere Regionen als Global müssen Sie zum Schutz von Ressourcen in mehreren Regionen eine separate Firewall Manager Manager-Richtlinie für jede Region erstellen.

6. Wählen Sie Weiter aus.
7. Geben Sie unter Name einen aussagekräftigen Namen ein.

8. Nur für Richtlinien für globale Regionen können Sie wählen, ob Sie die automatische DDoS-Abwehr auf Anwendungsebene mit Shield Advanced verwalten möchten. Informationen zu dieser Shield Advanced-Funktion finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#).

Sie können die automatische Schadensbegrenzung aktivieren oder deaktivieren oder sie ignorieren. Wenn Sie es ignorieren, verwaltet Firewall Manager die automatische Schadensbegrenzung für die Shield Advanced-Schutzmaßnahmen überhaupt nicht. Weitere Informationen zu diesen Richtlinienoptionen finden Sie unter [Automatische DDoS-Abwehr auf Anwendungsebene](#)

9. Wenn Sie möchten, dass Firewall Manager nicht verknüpfte Web-ACLs verwaltet, aktivieren Sie unter Web-ACLs verwalten die Option Nicht verknüpfte Web-ACLs verwalten. Mit dieser Option erstellt Firewall Manager Web-ACLs in den Konten innerhalb des Richtlinienbereichs nur dann, wenn die Web-ACLs von mindestens einer Ressource verwendet werden. Wenn ein Konto zu irgendeinem Zeitpunkt in den Geltungsbereich der Richtlinie fällt, erstellt Firewall Manager automatisch eine Web-ACL in dem Konto, sofern mindestens eine Ressource die Web-ACL verwendet. Nach der Aktivierung dieser Option führt Firewall Manager eine einmalige Bereinigung der nicht verknüpften Web-ACLs in Ihrem Konto durch. Der Bereinigungsprozess kann mehrere Stunden dauern. Wenn eine Ressource den Richtlinienbereich verlässt, nachdem Firewall Manager eine Web-ACL erstellt hat, trennt Firewall Manager die Ressource nicht von der Web-ACL. Um die Web-ACL in die einmalige Bereinigung einzubeziehen, müssen Sie zuerst die Ressourcen manuell von der Web-ACL trennen und dann die Option Nicht zugeordnete Web-ACLs verwalten aktivieren.
10. Für Richtlinienaktionen empfehlen wir, die Richtlinie mit der Option zu erstellen, dass nicht konforme Ressourcen nicht automatisch korrigiert werden. Wenn Sie die automatische Problembehebung deaktivieren, können Sie die Auswirkungen Ihrer neuen Richtlinie beurteilen, bevor Sie sie anwenden. Wenn Sie davon überzeugt sind, dass die Änderungen Ihren Wünschen entsprechen, bearbeiten Sie die Richtlinie und ändern Sie die Richtlinienaktion, um die automatische Korrektur zu aktivieren.

Wenn Sie die Richtlinie stattdessen automatisch auf vorhandene Ressourcen im Bereich anwenden möchten, wählen Sie Auto remediate any noncompliant resources (Alle nicht konformen Ressourcen automatisch korrigieren) aus. Diese Option wendet Shield Advanced-Schutzmaßnahmen für jedes entsprechende Konto innerhalb der AWS Organisation und jede entsprechende Ressource in den Konten an.

Wenn Sie bei Richtlinien für globale Regionen die Option Automatische Korrektur aller nicht konformen Ressourcen wählen, können Sie auch festlegen, dass Firewall Manager alle vorhandenen AWS WAF klassischen Web-ACLs automatisch durch neue Verknüpfungen zu Web-ACLs ersetzt, die mit der neuesten Version von AWS WAF (v2) erstellt wurden. Wenn Sie diese Option wählen, entfernt Firewall Manager die Verknüpfungen mit den Web-ACLs der früheren Version und erstellt neue Verknüpfungen mit Web-ACLs der neuesten Version, nachdem neue leere Web-ACLs in allen im Geltungsbereich befindlichen Konten erstellt wurden, für die sie noch nicht für die Richtlinie vorhanden sind. Weitere Informationen zu dieser Option finden Sie unter [Ersetzen Sie AWS WAF klassische Web-ACLs durch Web-ACLs der neuesten Version](#).

11. Wählen Sie Weiter aus.

12. Wenn AWS-Konten diese Richtlinie für gilt, wählen Sie die Option wie folgt aus:

- Wenn Sie die Richtlinie auf alle Konten in Ihrer Organisation anwenden möchten, behalten Sie die Standardauswahl Alle Konten meiner AWS Organisation einbeziehen bei.
- Wenn Sie die Richtlinie nur auf bestimmte Konten oder Konten in bestimmten AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Nur die angegebenen Konten und Organisationseinheiten einbeziehen aus und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie einbeziehen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.
- Wenn Sie die Richtlinie für alle Konten oder Organisationseinheiten (OUs) außer einer bestimmten Gruppe von Konten oder AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Die angegebenen Konten und Organisationseinheiten ausschließen und alle anderen einbeziehen aus, und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie ausschließen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

Sie können nur eine der Optionen auswählen.

Nachdem Sie die Richtlinie angewendet haben, bewertet Firewall Manager automatisch alle neuen Konten anhand Ihrer Einstellungen. Wenn Sie beispielsweise nur bestimmte Konten

angeben, wendet Firewall Manager die Richtlinie nicht auf neue Konten an. Ein weiteres Beispiel: Wenn Sie eine Organisationseinheit hinzufügen und der Organisationseinheit oder einer ihrer untergeordneten Organisationseinheiten ein Konto hinzufügen, wendet Firewall Manager die Richtlinie automatisch auf das neue Konto an.

13. Wählen Sie den Ressourcentyp aus, der geschützt werden soll.

Firewall Manager unterstützt Amazon Route 53 oder nicht AWS Global Accelerator. Wenn Sie Shield Advanced verwenden müssen, um Ressourcen vor diesen Diensten zu schützen, können Sie keine Firewall Manager Manager-Richtlinie verwenden. Folgen Sie stattdessen den Anweisungen von Shield Advanced unter [AWS Shield Advanced Schutz für Ressourcen hinzufügen AWS](#).

14. Wenn Sie nur Ressourcen mit bestimmten Tags schützen oder Ressourcen mit bestimmten Tags ausschließen möchten, wählen Sie „Tags zum Ein-/Ausschließen von Ressourcen verwenden“ aus, geben Sie die durch Kommas getrennten Tags ein und wählen Sie dann entweder „Einschließen“ oder „Ausschließen“. Sie können nur eine Option auswählen.

Wenn Sie mehr als ein Tag eingeben und eine Ressource über eines dieser Tags verfügt, wird dies als Übereinstimmung betrachtet.

Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).

15. Wählen Sie Weiter aus.
16. Fügen Sie für Policy-Tags alle Identifizierungs-Tags hinzu, die Sie für die Firewall Manager Manager-Richtlinie benötigen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).
17. Wählen Sie Weiter aus.
18. Überprüfen Sie die neue Richtlinie. Um Änderungen vorzunehmen, wählen Sie Edit (Bearbeiten) in dem Bereich, den Sie ändern möchten. Dadurch kehren Sie zum entsprechenden Schritt im Erstellungsassistenten zurück. Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen).

Erstellen einer gemeinsamen AWS Firewall Manager -Sicherheitsgruppenrichtlinie


Informationen zur Funktionsweise gemeinsamer Sicherheitsgruppenrichtlinien finden Sie unter [Gemeinsame Sicherheitsgruppenrichtlinien](#).

Um eine gemeinsame Sicherheitsgruppenrichtlinie zu erstellen, muss in Ihrem Firewall Manager Manager-Administratorkonto bereits eine Sicherheitsgruppe erstellt worden sein, die Sie als primäre

Gruppe für Ihre Richtlinie verwenden möchten. Sie können Sicherheitsgruppen über Amazon Virtual Private Cloud (Amazon VPC) oder Amazon Elastic Compute Cloud (Amazon EC2) verwalten. Weitere Informationen finden Sie unter [Arbeiten mit Sicherheitsgruppen](#) im [Amazon VPC-Benutzerhandbuch](#).


So erstellen Sie eine gemeinsame Sicherheitsgruppenrichtlinie (Konsole):

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

 Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie für Policy type (Richtlinientyp) die Option Security group (Sicherheitsgruppe).
5. Wählen Sie für Security group policy type (Sicherheitsgruppenrichtlinientyp) die Option Common security groups (Gemeinsame Sicherheitsgruppen) aus.
6. Wählen Sie für Region eine AWS-Region.
7. Wählen Sie Weiter aus.
8. Geben Sie unter Policy name (Richtliniennamen) einen Anzeigenamen ein.
9. Führen Sie für Policy rules (Richtlinienregeln), die folgenden Schritte aus:
 - a. Wählen Sie unter der Option Regeln die Einschränkungen aus, die Sie auf die Sicherheitsgruppenregeln und die Ressourcen anwenden möchten, die innerhalb des Richtlinienbereichs liegen. Wenn Sie Tags aus der primären Sicherheitsgruppe an die mit dieser Richtlinie erstellten Sicherheitsgruppen verteilen wählen, müssen Sie auch Identifizieren und melden auswählen, wenn die mit dieser Richtlinie erstellten Sicherheitsgruppen nicht mehr konform sind.

 Important

Firewall Manager verteilt keine von AWS Diensten hinzugefügten Systemtags an die Replikat-Sicherheitsgruppen. System-Tags beginnen mit dem Präfix aws :. Darüber

hinaus aktualisiert Firewall Manager die Tags vorhandener Sicherheitsgruppen nicht und erstellt auch keine neuen Sicherheitsgruppen, wenn die Richtlinie Tags enthält, die mit der Tag-Richtlinie der Organisation in Konflikt stehen. Informationen zu Tag-Richtlinien finden Sie unter [Tag-Richtlinien](#) im AWS Organizations Benutzerhandbuch.

Wenn Sie die Option Sicherheitsgruppenreferenzen von der primären Sicherheitsgruppe an die mit dieser Richtlinie erstellten Sicherheitsgruppen verteilen wählen, verteilt Firewall Manager die Sicherheitsgruppenreferenzen nur, wenn sie über eine aktive Peering-Verbindung in Amazon VPC verfügen. Informationen zu dieser Option finden Sie unter Einstellungen für [Richtlinienregeln](#).

- b. Wählen Sie für Primäre Sicherheitsgruppen die Option Primäre Sicherheitsgruppe hinzufügen und wählen Sie dann die Sicherheitsgruppe aus, die Sie verwenden möchten. Firewall Manager füllt die Liste der primären Sicherheitsgruppen aus allen Amazon VPC-Instances im Firewall Manager Manager-Administratorkonto aus. Der Standardgrenzwert für die Anzahl der primären Sicherheitsgruppen für eine Richtlinie ist eine. Informationen zum Erhöhen des Maximalwerts finden Sie unter [AWS Firewall Manager Kontingente](#).
- c. Für Policy action (Richtlinienaktion) empfehlen wir, die Richtlinie mit der Option zu erstellen, die nicht automatisch korrigiert wird. Auf diese Weise können Sie die Auswirkungen Ihrer neuen Richtlinie prüfen, bevor Sie sie anwenden. Wenn Sie sich sicher sind, dass die Änderungen Ihren Wünschen entsprechen, bearbeiten Sie die Richtlinie und ändern Sie die Richtlinienaktion, um die automatische Korrektur nicht konformer Ressourcen zu aktivieren.

10. Wählen Sie Weiter aus.

11. Wenn AWS-Konten diese Richtlinie gilt für, wählen Sie die Option wie folgt aus:

- Wenn Sie die Richtlinie auf alle Konten in Ihrer Organisation anwenden möchten, behalten Sie die Standardauswahl Alle Konten meiner AWS Organisation einbeziehen bei.
- Wenn Sie die Richtlinie nur auf bestimmte Konten oder Konten in bestimmten AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Nur die angegebenen Konten und Organisationseinheiten einbeziehen aus und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie einbeziehen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

- Wenn Sie die Richtlinie für alle Konten oder Organisationseinheiten (OUs) außer einer bestimmten Gruppe von Konten oder AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Die angegebenen Konten und Organisationseinheiten ausschließen und alle anderen einbeziehen aus, und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie ausschließen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

Sie können nur eine der Optionen auswählen.


Nachdem Sie die Richtlinie angewendet haben, bewertet Firewall Manager automatisch alle neuen Konten anhand Ihrer Einstellungen. Wenn Sie beispielsweise nur bestimmte Konten angeben, wendet Firewall Manager die Richtlinie nicht auf neue Konten an. Ein weiteres Beispiel: Wenn Sie eine Organisationseinheit hinzufügen und der Organisationseinheit oder einer ihrer untergeordneten Organisationseinheiten ein Konto hinzufügen, wendet Firewall Manager die Richtlinie automatisch auf das neue Konto an.

12. Wählen Sie unter Resource type (Ressourcentyp) die Arten von Ressourcen aus, die Sie schützen möchten.

Wenn Sie sich für eine EC2-Instance entscheiden, können Sie wählen, ob alle Elastic Network-Schnittstellen in jede Amazon EC2 EC2-Instance oder nur die Standardschnittstelle in jeder Instance aufgenommen werden sollen. Wenn Sie mehr als eine elastic network interface in einer Amazon EC2 EC2-Instance im Geltungsbereich haben, kann Firewall Manager die Richtlinie auf alle anwenden, wenn Sie die Option zum Einbeziehen aller Schnittstellen wählen. Wenn Sie die automatische Problembeseitigung aktivieren und Firewall Manager die Richtlinie nicht auf alle Elastic Network-Schnittstellen in einer Amazon EC2 EC2-Instance anwenden kann, markiert er die Instance als nicht konform.

13. Wenn Sie die Richtlinie für alle Ressourcen innerhalb der Parameter AWS-Konten und Ressourcentyp anwenden möchten, wählen Sie unter Ressourcen die Option Alle Ressourcen einbeziehen, die dem ausgewählten Ressourcentyp entsprechen. Wenn Sie bestimmte Ressourcen einschließen oder ausschließen möchten, geben Sie die Ressourcen mithilfe von Tagging an. Wählen Sie dann die entsprechende Option aus und fügen Sie die Tags der Liste hinzu. Sie können die Richtlinie entweder auf alle Ressourcen anwenden, außer auf diejenigen, die über alle von Ihnen angegebenen Tags verfügen, oder Sie können sie nur auf diejenigen

anwenden, die über alle von Ihnen angegebenen Tags verfügen. Weitere Informationen zum Kennzeichnen Ihrer Ressourcen finden Sie unter [Arbeiten mit Tag-Editor](#).

 Note

Wenn Sie mehr als ein Tag eingeben, muss eine Ressource über alle Tags verfügen, um eine Übereinstimmung zu bieten.

14. Wenn Sie in Shared VPC resources (Freigegebene VPC-Ressourcen) die Richtlinie auf Ressourcen in freigegebenen VPCs anwenden möchten, wählen Sie zusätzlich zu den VPCs, die die Konten besitzen, die Option Include resources from shared VPCs (Ressourcen aus freigegebenen VPCs einschließen) aus.
15. Wählen Sie Weiter aus.
16. Überprüfen Sie die Richtlinieneinstellungen, um sicherzustellen, dass sie Ihren Wünschen entsprechen, und wählen Sie dann Create policy (Richtlinie erstellen).

Firewall Manager erstellt ein Replikat der primären Sicherheitsgruppe in jeder Amazon VPC-Instance, die innerhalb der im Geltungsbereich enthaltenen Konten enthalten ist, bis zu dem unterstützten maximalen Amazon VPC-Kontingent pro Konto. Firewall Manager ordnet die Replikat-Sicherheitsgruppen den Ressourcen zu, die innerhalb des Richtlinienbereichs für jedes in den Geltungsbereich fallende Konto liegen. Weitere Information zur Funktionsweise dieser Richtlinie finden Sie unter [Gemeinsame Sicherheitsgruppenrichtlinien](#).

Erstellen einer AWS Firewall Manager -Inhaltsprüfungssicherheitsgruppenrichtlinie

Informationen zur Funktionsweise der Inhaltsprüfungssicherheitsgruppenrichtlinie finden Sie unter [Inhaltsprüfungssicherheitsgruppenrichtlinien](#).

Für einige Einstellungen der Inhaltsüberwachungsrichtlinie müssen Sie eine Überwachungssicherheitsgruppe angeben, die Firewall Manager als Vorlage verwenden kann. Möglicherweise haben Sie eine Audit-Sicherheitsgruppe, die alle Regeln enthält, die Sie in keiner Sicherheitsgruppe zulassen. Sie müssen diese Audit-Sicherheitsgruppen mit Ihrem Firewall Manager-Administratorkonto erstellen, bevor Sie sie in Ihrer Richtlinie verwenden können. Sie können Sicherheitsgruppen über Amazon Virtual Private Cloud (Amazon VPC) oder Amazon Elastic Compute Cloud (Amazon EC2) verwalten. Weitere Informationen finden Sie unter [Arbeiten mit Sicherheitsgruppen](#) im [Amazon VPC-Benutzerhandbuch](#).

So erstellen Sie eine Inhaltsprüfungssicherheitsgruppenrichtlinie (Konsole)

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Administratorkonto an und öffnen Sie dann die Firewall Manager Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie für Policy type (Richtlinientyp) die Option Security group (Sicherheitsgruppe).
5. Wählen Sie für Security group policy type (Sicherheitsgruppenrichtlinientyp) die Option Auditing and enforcement of security group rules (Überwachung und Durchsetzung von Sicherheitsgruppenregeln).
6. Wählen Sie für Region eine AWS-Region.
7. Wählen Sie Weiter aus.
8. Geben Sie unter Policy name (Richtliniennamen) einen Anzeigenamen ein.
9. Wählen Sie unter Richtlinienregeln die Option für verwaltete oder benutzerdefinierte Richtlinienregeln aus, die Sie verwenden möchten.
 - a. Gehen Sie unter „Regeln für verwaltete Überwachungsrichtlinien konfigurieren“ wie folgt vor:
 - i. Wählen Sie unter Sicherheitsgruppenregeln für die Überwachung konfigurieren den Typ der Sicherheitsgruppenregeln aus, für die Ihre Überwachungsrichtlinie gelten soll.
 - ii. Wenn Sie beispielsweise Regeln auf der Grundlage der Protokolle, Ports und CIDR-Bereichseinstellungen in Ihren Sicherheitsgruppen überprüfen möchten, wählen Sie Übermäßig zulässige Sicherheitsgruppenregeln überwachen und wählen Sie die gewünschten Optionen aus.

Für die Auswahlregel lässt den gesamten Datenverkehr zu, können Sie eine benutzerdefinierte Anwendungsliste angeben, um die Anwendungen festzulegen, die Sie überwachen möchten. Informationen zu benutzerdefinierten Anwendungslisten und

deren Verwendung in Ihrer Richtlinie finden Sie unter [Verwaltete Listen](#) und [Verwenden von verwalteten Listen](#).

Für Auswahlen, die Protokolllisten verwenden, können Sie vorhandene Listen verwenden und neue Listen erstellen. Informationen zu Protokolllisten und deren Verwendung in Ihrer Richtlinie finden Sie unter [Verwaltete Listen](#) und [Verwenden von verwalteten Listen](#).

- iii. Wenn Sie hochriskante Anwendungen auf der Grundlage ihres Zugriffs auf reservierte oder nicht reservierte CIDR-Bereiche prüfen möchten, wählen Sie Anwendungen mit hohem Risiko prüfen und wählen Sie die gewünschten Optionen aus.

Die folgenden Auswahlmöglichkeiten schließen sich gegenseitig aus: Anwendungen, die nur auf reservierte CIDR-Bereiche zugreifen können, und Anwendungen, denen der Zugriff auf nicht reservierte CIDR-Bereiche gestattet ist. Sie können in jeder Richtlinie höchstens eine davon auswählen.

Für Auswahlen, die Anwendungslisten verwenden, können Sie vorhandene Listen verwenden und neue Listen erstellen. Informationen zu Anwendungslisten und deren Verwendung in Ihrer Richtlinie finden Sie unter [Verwaltete Listen](#) und [Verwenden von verwalteten Listen](#).

- iv. Verwenden Sie die Einstellungen für Außerkräftsetzungen, um andere Einstellungen in der Richtlinie explizit zu überschreiben. Sie können festlegen, dass bestimmte Sicherheitsgruppenregeln immer zugelassen oder verweigert werden, unabhängig davon, ob sie den anderen Optionen entsprechen, die Sie für die Richtlinie festgelegt haben.

Für diese Option geben Sie eine Audit-Sicherheitsgruppe als Vorlage für zulässige Regeln oder verweigerter Regeln an. Wählen Sie für Überwachungssicherheitsgruppen die Option Auditsicherheitsgruppen hinzufügen und wählen Sie dann die Sicherheitsgruppe aus, die Sie verwenden möchten. Firewall Manager füllt die Liste der Audit-Sicherheitsgruppen aus allen Amazon VPC-Instances im Firewall Manager Administratorkonto aus. Das standardmäßige Höchstkontingent für die Anzahl der Überwachungssicherheitsgruppen für eine Richtlinie ist eine. Informationen zum Erhöhen des Kontingents finden Sie unter [AWS Firewall Manager Kontingente](#).

- b. Gehen Sie wie folgt vor, um benutzerdefinierte Richtlinienregeln zu konfigurieren:
 - i. Wählen Sie aus den Regeloptionen aus, ob nur die Regeln zugelassen werden sollen, die in den Prüfungssicherheitsgruppen definiert sind, oder ob alle Regeln

abgelehnt werden sollen. Weitere Informationen zu dieser Auswahl finden Sie unter [Inhaltsprüfungssicherheitsgruppenrichtlinien](#).

- ii. Wählen Sie für Audit-Sicherheitsgruppen die Option Audit-Sicherheitsgruppen hinzufügen und wählen Sie dann die Sicherheitsgruppe aus, die Sie verwenden möchten. Firewall Manager füllt die Liste der Audit-Sicherheitsgruppen aus allen Amazon VPC-Instances im Firewall Manager Manager-Administratorkonto aus. Das standardmäßige Höchstkontingent für die Anzahl der Überwachungssicherheitsgruppen für eine Richtlinie ist eine. Informationen zum Erhöhen des Kontingents finden Sie unter [AWS Firewall Manager Kontingente](#).
- iii. Für Policy action (Richtlinienaktion) müssen Sie die Richtlinie mit der Option erstellen, die nicht automatisch korrigiert wird. Auf diese Weise können Sie die Auswirkungen Ihrer neuen Richtlinie prüfen, bevor Sie sie anwenden. Wenn Sie sich sicher sind, dass die Änderungen Ihren Wünschen entsprechen, bearbeiten Sie die Richtlinie und ändern Sie die Richtlinienaktion, um die automatische Korrektur nicht konformer Ressourcen zu aktivieren.

10. Wählen Sie Weiter aus.


11. Wenn AWS-Konten diese Richtlinie gilt für, wählen Sie die Option wie folgt aus:

- Wenn Sie die Richtlinie auf alle Konten in Ihrer Organisation anwenden möchten, behalten Sie die Standardauswahl Alle Konten meiner AWS Organisation einbeziehen bei.
- Wenn Sie die Richtlinie nur auf bestimmte Konten oder Konten in bestimmten AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Nur die angegebenen Konten und Organisationseinheiten einbeziehen aus und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie einbeziehen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.
- Wenn Sie die Richtlinie für alle Konten oder Organisationseinheiten (OUs) außer einer bestimmten Gruppe von Konten oder AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Die angegebenen Konten und Organisationseinheiten ausschließen und alle anderen einbeziehen aus, und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie ausschließen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

Sie können nur eine der Optionen auswählen.

Nachdem Sie die Richtlinie angewendet haben, bewertet Firewall Manager automatisch alle neuen Konten anhand Ihrer Einstellungen. Wenn Sie beispielsweise nur bestimmte Konten angeben, wendet Firewall Manager die Richtlinie nicht auf neue Konten an. Ein weiteres Beispiel: Wenn Sie eine Organisationseinheit hinzufügen und der Organisationseinheit oder einer ihrer untergeordneten Organisationseinheiten ein Konto hinzufügen, wendet Firewall Manager die Richtlinie automatisch auf das neue Konto an.

12. Wählen Sie unter Resource type (Ressourcentyp) die Ressourcentypen aus, die Sie schützen möchten.
13. Wenn Sie die Richtlinie für alle Ressourcen innerhalb der Parameter AWS-Konten und Ressourcentyp anwenden möchten, wählen Sie unter Ressourcen die Option Alle Ressourcen einbeziehen, die dem ausgewählten Ressourcentyp entsprechen. Wenn Sie bestimmte Ressourcen einschließen oder ausschließen möchten, geben Sie die Ressourcen mithilfe von Tagging an. Wählen Sie dann die entsprechende Option aus und fügen Sie die Tags der Liste hinzu. Sie können die Richtlinie entweder auf alle Ressourcen anwenden, außer auf diejenigen, die über alle von Ihnen angegebenen Tags verfügen, oder Sie können sie nur auf diejenigen anwenden, die über alle von Ihnen angegebenen Tags verfügen. Weitere Informationen zum Kennzeichnen Ihrer Ressourcen finden Sie unter [Arbeiten mit Tag-Editor](#).

 Note

Wenn Sie mehr als ein Tag eingeben, muss eine Ressource über alle Tags verfügen, um eine Übereinstimmung zu bieten.

14. Wählen Sie Weiter aus.
15. Überprüfen Sie die Richtlinieneinstellungen, um sicherzustellen, dass sie Ihren Wünschen entsprechen, und wählen Sie dann Create policy (Richtlinie erstellen).

Firewall Manager vergleicht die Audit-Sicherheitsgruppe gemäß Ihren Richtlinienregeleinstellungen mit den im Geltungsbereich enthaltenen Sicherheitsgruppen in Ihrer AWS Organisation. Sie können den Status der Richtlinie in der AWS Firewall Manager Richtlinienkonsole überprüfen. Nachdem die Richtlinie erstellt wurde, können Sie sie bearbeiten und die automatische Standardisierung aktivieren, um die Prüfungssicherheitsgruppenrichtlinie in Kraft zu setzen. Weitere Information zur Funktionsweise dieser Richtlinie finden Sie unter [Inhaltsprüfungssicherheitsgruppenrichtlinien](#).

Erstellen einer AWS Firewall Manager -Nutzungsprüfungssicherheitsgruppenrichtlinie

Weitere Informationen zur Funktionsweise von Nutzungsprüfungssicherheitsgruppenrichtlinien finden Sie unter [Nutzungsprüfungssicherheitsgruppenrichtlinien](#).

So erstellen Sie eine Nutzungsprüfungssicherheitsgruppenrichtlinie (Konsole):


1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).


2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie für Policy type (Richtlinientyp) die Option Security group (Sicherheitsgruppe).
5. Wählen Sie als Gruppenrichtlinientyp die Option Überwachung und Säuberung nicht zugeordneter und redundanter Sicherheitsgruppen aus.
6. Wählen Sie für Region eine aus. AWS-Region
7. Wählen Sie Weiter aus.
8. Geben Sie unter Policy name (Richtliniennamen) einen Anzeigenamen ein.
9. Wählen Sie für Policy rules (Richtlinienregeln) eine oder beide der verfügbaren Optionen aus.
 - Wenn Sie die Option Sicherheitsgruppen innerhalb dieses Richtlinienbereichs müssen von mindestens einer Ressource verwendet werden wählen, entfernt Firewall Manager alle Sicherheitsgruppen, die er für unbenutzt hält. Wenn diese Regel aktiviert ist, führt Firewall Manager sie zuletzt aus, wenn Sie die Richtlinie speichern.

Einzelheiten dazu, wie Firewall Manager die Nutzung und den Zeitpunkt der Behebung bestimmt, finden Sie unter [Nutzungsprüfungssicherheitsgruppenrichtlinien](#).

 Note

Wenn Sie diesen Sicherheits-Gruppenrichtlinientyp „Nutzungsüberwachung“ verwenden, vermeiden Sie es, innerhalb kurzer Zeit mehrere Änderungen am Zuordnungsstatus der in den Geltungsbereich fallenden Sicherheitsgruppen vorzunehmen. Dies kann dazu führen, dass Firewall Manager entsprechende Ereignisse verpasst.

Standardmäßig betrachtet Firewall Manager Sicherheitsgruppen als nicht konform mit dieser Richtlinienregel, sobald sie nicht verwendet werden. Sie können optional eine Anzahl von Minuten angeben, für die eine Sicherheitsgruppe ungenutzt bestehen kann, bevor sie als nicht konform eingestuft wird, nämlich bis zu 525.600 Minuten (365 Tage). Sie können diese Einstellung verwenden, um sich Zeit zu nehmen, um neue Sicherheitsgruppen Ressourcen zuzuordnen.

 Important

Wenn Sie eine andere Anzahl von Minuten als den Standardwert Null angeben, müssen Sie indirekte Beziehungen in aktivieren AWS Config. Andernfalls funktionieren Ihre Sicherheitsgruppenrichtlinien für die Nutzungsüberwachung nicht wie vorgesehen. Informationen zu indirekten Beziehungen finden Sie unter [Indirekte Beziehungen AWS Config im AWS Config](#) Entwicklerhandbuch. AWS Config


- Wenn Sie die Option Sicherheitsgruppen innerhalb dieses Richtlinienbereichs müssen eindeutig sein wählen, konsolidiert Firewall Manager redundante Sicherheitsgruppen, sodass jeder Ressource nur eine zugeordnet ist. Wenn Sie diese Option wählen, führt Firewall Manager sie zuerst aus, wenn Sie die Richtlinie speichern.
10. Für Policy action (Richtlinienaktion) empfehlen wir, die Richtlinie mit der Option zu erstellen, die nicht automatisch korrigiert wird. Auf diese Weise können Sie die Auswirkungen Ihrer neuen Richtlinie prüfen, bevor Sie sie anwenden. Wenn Sie sich sicher sind, dass die Änderungen Ihren Wünschen entsprechen, bearbeiten Sie die Richtlinie und ändern Sie die Richtlinienaktion, um die automatische Korrektur nicht konformer Ressourcen zu aktivieren.
 11. Wählen Sie Weiter aus.
 12. Wenn AWS-Konten diese Richtlinie für gilt, wählen Sie die Option wie folgt aus:

- Wenn Sie die Richtlinie auf alle Konten in Ihrer Organisation anwenden möchten, behalten Sie die Standardauswahl Alle Konten meiner AWS Organisation einbeziehen bei.
- Wenn Sie die Richtlinie nur auf bestimmte Konten oder Konten in bestimmten AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Nur die angegebenen Konten und Organisationseinheiten einbeziehen aus und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie einbeziehen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.
- Wenn Sie die Richtlinie für alle Konten oder Organisationseinheiten (OUs) außer einer bestimmten Gruppe von Konten oder AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Die angegebenen Konten und Organisationseinheiten ausschließen und alle anderen einbeziehen aus, und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie ausschließen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

Sie können nur eine der Optionen auswählen.

Nachdem Sie die Richtlinie angewendet haben, bewertet Firewall Manager automatisch alle neuen Konten anhand Ihrer Einstellungen. Wenn Sie beispielsweise nur bestimmte Konten angeben, wendet Firewall Manager die Richtlinie nicht auf neue Konten an. Ein weiteres Beispiel: Wenn Sie eine Organisationseinheit hinzufügen und der Organisationseinheit oder einer ihrer untergeordneten Organisationseinheiten ein Konto hinzufügen, wendet Firewall Manager die Richtlinie automatisch auf das neue Konto an.

13. Wenn Sie die Richtlinie für alle Ressourcen innerhalb der Parameter AWS-Konten und Ressourcentyp anwenden möchten, wählen Sie unter Ressourcen die Option Alle Ressourcen einbeziehen, die dem ausgewählten Ressourcentyp entsprechen. Wenn Sie bestimmte Ressourcen einschließen oder ausschließen möchten, geben Sie die Ressourcen mithilfe von Tagging an. Wählen Sie dann die entsprechende Option aus und fügen Sie die Tags der Liste hinzu. Sie können die Richtlinie entweder auf alle Ressourcen anwenden, außer auf diejenigen, die über alle von Ihnen angegebenen Tags verfügen, oder Sie können sie nur auf diejenigen anwenden, die über alle von Ihnen angegebenen Tags verfügen. Weitere Informationen zum Kennzeichnen Ihrer Ressourcen finden Sie unter [Arbeiten mit Tag-Editor](#).

 Note

Wenn Sie mehr als ein Tag eingeben, muss eine Ressource über alle Tags verfügen, um eine Übereinstimmung zu bieten.

14. Wählen Sie Weiter aus.
15. Wenn Sie das Firewall Manager-Administratorkonto nicht aus dem Richtlinienbereich ausgeschlossen haben, werden Sie von Firewall Manager dazu aufgefordert. Dadurch bleiben die Sicherheitsgruppen im Firewall Manager Manager-Administratorkonto, das Sie für allgemeine Sicherheitsgruppenrichtlinien und Überwachungsrichtlinien verwenden, unter Ihrer manuellen Kontrolle. Wählen Sie in diesem Dialog die gewünschte Option aus.
16. Überprüfen Sie die Richtlinieneinstellungen, um sicherzustellen, dass sie Ihren Wünschen entsprechen, und wählen Sie dann Create policy (Richtlinie erstellen).

Wenn Sie sich dafür entschieden haben, eindeutige Sicherheitsgruppen vorzuschreiben, sucht Firewall Manager in jeder Amazon VPC-Instance im Geltungsbereich nach redundanten Sicherheitsgruppen. Wenn Sie dann festlegen, dass jede Sicherheitsgruppe von mindestens einer Ressource verwendet werden muss, sucht Firewall Manager nach Sicherheitsgruppen, die für die in der Regel angegebenen Minuten ungenutzt geblieben sind. Sie können den Status der Richtlinie in der AWS Firewall Manager Richtlinienkonsole überprüfen. Weitere Informationen zur Funktionsweise dieser Richtlinie finden Sie unter [Nutzungsprüfungssicherheitsgruppenrichtlinien](#).


Eine AWS Firewall Manager Richtlinie erstellen für AWS Network Firewall

In einer Firewall Manager Manager-Netzwerk-Firewall-Richtlinie verwenden Sie Regelgruppen, in denen Sie verwalten AWS Network Firewall. Informationen zur Verwaltung Ihrer Regelgruppen finden Sie unter [AWS Network Firewall Regelgruppen](#) im Network Firewall Developer Guide.

Informationen zu den Netzwerk-Firewall-Richtlinien von Firewall Manager finden Sie unter [AWS Network Firewall Richtlinien](#).

So erstellen Sie eine Firewall Manager Manager-Richtlinie für AWS Network Firewall (Konsole)

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

 Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie unter Policy type (Richtlinientyp) die Option AWS Network Firewall.
5. Wählen Sie unter Firewall-Management-Typ aus, wie Firewall Manager die Firewalls der Richtlinie verwalten soll. Wählen Sie aus den folgenden Optionen aus:
 - Verteilt — Firewall Manager erstellt und verwaltet Firewall-Endpunkte in jeder VPC, die im Richtlinienbereich enthalten sind.
 - Zentralisiert — Firewall Manager erstellt und verwaltet Endpoints in einer einzigen Inspektions-VPC.
 - Importieren vorhandener Firewalls — Firewall Manager importiert vorhandene Firewalls mithilfe von Ressourcensätzen aus der Network Firewall. Informationen zu Ressourcensätzen finden Sie unter [Arbeiten mit Ressourcensätzen in Firewall Manager](#)
6. Wählen Sie für Region eine AWS-Region. Um Ressourcen in mehreren Regionen zu schützen, müssen Sie für jede Region separate Richtlinien erstellen.
7. Wählen Sie Weiter aus.
8. Geben Sie als Richtlinienname einen aussagekräftigen Namen ein. Firewall Manager nimmt den Richtliniennamen in die Namen der Netzwerk-Firewall-Firewalls und der Firewall-Richtlinien auf, die er erstellt.
9. Konfigurieren Sie in der AWS Network Firewall Richtlinienkonfiguration die Firewall-Richtlinie wie in der Network Firewall. Fügen Sie Ihre statusfreien und statusbehafteten Regelgruppen hinzu und geben Sie die Standardaktionen der Richtlinie an. Sie können optional die Reihenfolge der Statusregelauswertung und die Standardaktionen der Richtlinie sowie die Protokollierungskonfiguration festlegen. Informationen zur Verwaltung von Firewall-Richtlinien für [AWS Network Firewall Netzwerkfirewalls](#) finden Sie unter [Firewallrichtlinien](#) im AWS Network Firewall Entwicklerhandbuch.


Wenn Sie die Firewall Manager-Netzwerk-Firewall-Richtlinie erstellen, erstellt Firewall Manager Firewall-Richtlinien für die Konten, die in den Geltungsbereich fallen. Einzelne Kontomanager

können Regelgruppen zu den Firewall-Richtlinien hinzufügen, aber sie können die Konfiguration, die Sie hier angeben, nicht ändern.

10. Wählen Sie Weiter aus.

11. Führen Sie je nach dem Firewall-Verwaltungstyp, den Sie im vorherigen Schritt ausgewählt haben, einen der folgenden Schritte aus:


- Wenn Sie einen verteilten Firewall-Managementtyp verwenden, wählen Sie in der AWS Firewall Manager Endpunktconfiguration unter Standort des Firewall-Endpunkts eine der folgenden Optionen aus:
 - Benutzerdefinierte Endpunktconfiguration — Firewall Manager erstellt Firewalls für jede VPC innerhalb des Richtlinienbereichs in den von Ihnen angegebenen Availability Zones. Jede Firewall enthält mindestens einen Firewall-Endpunkt.
 - Wählen Sie unter Availability Zones aus, in welchen Availability Zones Firewall-Endpoints erstellt werden sollen. Sie können Availability Zones nach dem Namen der Availability Zone oder nach der Availability Zone ID auswählen.
 - Wenn Sie die CIDR-Blöcke für Firewall Manager zur Verwendung für Firewall-Subnetze in Ihren VPCs bereitstellen möchten, müssen sie alle /28 CIDR-Blöcke sein. Geben Sie einen Block pro Zeile ein. Wenn Sie diese weglassen, wählt Firewall Manager IP-Adressen für Sie aus den in den VPCs verfügbaren IP-Adressen aus.

 Note

Die automatische Korrektur erfolgt automatisch für AWS Firewall Manager Netzwerk-Firewall-Richtlinien, sodass Sie hier keine Option sehen, die auto Korrektur abzulehnen.

- Automatische Endpunktconfiguration — Firewall Manager erstellt automatisch Firewall-Endpunkte in den Availability Zones mit öffentlichen Subnetzen in Ihrer VPC.
 - Geben Sie für die Konfiguration der Firewall-Endpunkte an, wie die Firewall-Endpunkte von Firewall Manager verwaltet werden sollen. Wir empfehlen die Verwendung mehrerer Endpunkte für eine hohe Verfügbarkeit.
- Wenn Sie einen zentralen Firewall-Managementtyp verwenden, geben Sie in der AWS Firewall Manager Endpunktconfiguration unter Inspektion-VPC-Konfiguration die AWS Konto-ID des Besitzers der Inspektion-VPC und die VPC-ID der Inspektion-VPC ein.

- Wählen Sie unter Availability Zones aus, in welchen Availability Zones Firewall-Endpoints erstellt werden sollen. Sie können Availability Zones nach dem Namen der Availability Zone oder nach der Availability Zone ID auswählen.
- Wenn Sie die CIDR-Blöcke für Firewall Manager zur Verwendung für Firewall-Subnetze in Ihren VPCs bereitstellen möchten, müssen sie alle /28 CIDR-Blöcke sein. Geben Sie einen Block pro Zeile ein. Wenn Sie diese weglassen, wählt Firewall Manager IP-Adressen für Sie aus den in den VPCs verfügbaren IP-Adressen aus.


 Note

Die automatische Korrektur erfolgt automatisch für AWS Firewall Manager Netzwerk-Firewall-Richtlinien, sodass Sie hier keine Option sehen, die auto Korrektur abzulehnen.

- Wenn Sie den Firewall-Managementtyp „Bestehende Firewalls importieren“ verwenden, fügen Sie unter Ressourcensätze eine oder mehrere Ressourcensätze hinzu. Ein Ressourcensatz definiert die vorhandenen Netzwerk-Firewall-Firewalls, die dem Konto Ihrer Organisation gehören und die Sie in dieser Richtlinie zentral verwalten möchten. Um der Richtlinie einen Ressourcensatz hinzuzufügen, müssen Sie zunächst mithilfe der Konsole oder der [PutResourceSet](#) API einen Ressourcensatz erstellen. Informationen zu Ressourcensätzen finden Sie unter [Arbeiten mit Ressourcensätzen in Firewall Manager](#). Weitere Informationen zum Importieren vorhandener Firewalls aus der Network Firewall finden Sie unter [Importieren vorhandener Firewalls](#).

12. Wählen Sie Weiter aus.

13. Wenn Ihre Richtlinie einen verteilten Firewallverwaltungstyp verwendet, wählen Sie unter Routenverwaltung aus, ob Firewall Manager den Datenverkehr, der durch die jeweiligen Firewallendpunkte geleitet werden muss, überwacht und Warnmeldungen dazu sendet.

 Note

Wenn Sie „Überwachen“ wählen, können Sie die Einstellung zu einem späteren Zeitpunkt nicht auf Aus ändern. Die Überwachung wird fortgesetzt, bis Sie die Richtlinie löschen.

14. Fügen Sie als Verkehrstyp optional die Datenverkehrsendpunkte hinzu, über die Sie den Datenverkehr zur Firewall-Inspektion weiterleiten möchten.

15. Wenn Sie diese Option für Allow required cross-AZ traffic aktivieren, behandelt Firewall Manager Availability Zones, die keinen eigenen Firewall-Endpunkt haben, als konformes Routing, das Datenverkehr aus einer Availability Zone zur Überprüfung sendet. Availability Zones mit Endpunkten müssen immer ihren eigenen Datenverkehr überprüfen.
16. Wählen Sie Weiter aus.
17. Wählen Sie für den Geltungsbereich der Richtlinie unter AWS-Konten Diese Richtlinie gilt für die folgende Option aus:
 - Wenn Sie die Richtlinie auf alle Konten in Ihrer Organisation anwenden möchten, behalten Sie die Standardauswahl Alle Konten meiner AWS Organisation einbeziehen bei.
 - Wenn Sie die Richtlinie nur auf bestimmte Konten oder Konten in bestimmten AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Nur die angegebenen Konten und Organisationseinheiten einbeziehen aus und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie einbeziehen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.
 - Wenn Sie die Richtlinie für alle Konten oder Organisationseinheiten (OUs) außer einer bestimmten Gruppe von Konten oder AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Die angegebenen Konten und Organisationseinheiten ausschließen und alle anderen einbeziehen aus, und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie ausschließen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

Sie können nur eine der Optionen auswählen.

Nachdem Sie die Richtlinie angewendet haben, bewertet Firewall Manager automatisch alle neuen Konten anhand Ihrer Einstellungen. Wenn Sie beispielsweise nur bestimmte Konten angeben, wendet Firewall Manager die Richtlinie nicht auf neue Konten an. Ein weiteres Beispiel: Wenn Sie eine Organisationseinheit hinzufügen und der Organisationseinheit oder einer ihrer untergeordneten Organisationseinheiten ein Konto hinzufügen, wendet Firewall Manager die Richtlinie automatisch auf das neue Konto an.

18. Der Ressourcentyp für Netzwerk-Firewall-Richtlinien ist VPC.

19. Wenn Sie unter Resources (Ressourcen) nur Ressourcen schützen (oder ausschließen) möchten, die bestimmte Tags haben, wählen Sie die entsprechende Option aus und geben Sie dann die Tags ein, die eingeschlossen oder ausgeschlossen werden sollen. Sie können nur eine Option auswählen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).

Wenn Sie mehrere Tags eingeben, muss eine Ressource über alle Tags verfügen, die eingeschlossen oder ausgeschlossen werden sollen.

20. Wählen Sie Weiter aus.

21. Fügen Sie für Policy-Tags alle Identifizierungs-Tags hinzu, die Sie für die Firewall Manager Manager-Richtlinie benötigen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).

22. Wählen Sie Weiter aus.

23. Überprüfen Sie die neue Richtlinie. Um Änderungen vorzunehmen, wählen Sie Edit (Bearbeiten) in dem Bereich, den Sie ändern möchten. Dadurch kehren Sie zum entsprechenden Schritt im Erstellungsassistenten zurück. Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen).


Erstellen einer AWS Firewall Manager Richtlinie für Amazon Route 53 Resolver DNS Firewall

In einer Firewall Manager DNS-Firewall-Richtlinie verwenden Sie Regelgruppen, die Sie in Amazon Route 53 Resolver DNS Firewall verwalten. Informationen zur Verwaltung Ihrer Regelgruppen finden Sie unter [Verwaltung von Regelgruppen und Regeln in der DNS-Firewall](#) im Amazon Route 53 Developer Guide.

Informationen zu den DNS-Firewallrichtlinien von Firewall Manager finden Sie unter [DNS-Firewall-Richtlinien für Amazon Route 53 Resolver](#).

So erstellen Sie eine Firewall Manager Manager-Richtlinie für Amazon Route 53 Resolver DNS Firewall (Konsole)

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

 Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie als Richtlinientyp die Option Amazon Route 53 Resolver DNS-Firewall aus.
5. Wählen Sie für Region eine AWS-Region. Um Ressourcen in mehreren Regionen zu schützen, müssen Sie für jede Region separate Richtlinien erstellen.
6. Wählen Sie Weiter aus.
7. Geben Sie als Richtliniennamen einen aussagekräftigen Namen ein.
8. Fügen Sie in der Richtlinienkonfiguration die Regelgruppen hinzu, die die DNS-Firewall unter den Regelgruppenzuordnungen Ihrer VPCs an erster und letzter Stelle auswerten soll. Sie können der Richtlinie bis zu zwei Regelgruppen hinzufügen.

Wenn Sie die DNS-Firewall-Richtlinie von Firewall Manager erstellen, erstellt Firewall Manager die Regelgruppenzuordnungen mit den von Ihnen angegebenen Zuordnungsprioritäten für die VPCs und Konten, die innerhalb des Gültigkeitsbereichs liegen. Die einzelnen Kontomanager können Regelgruppenzuordnungen zwischen Ihrer ersten und letzten Zuordnung hinzufügen, aber sie können die Zuordnungen, die Sie hier definieren, nicht ändern. Weitere Informationen finden Sie unter [DNS-Firewall-Richtlinien für Amazon Route 53 Resolver](#).

9. Wählen Sie Weiter.
10. Wenn AWS-Konten diese Richtlinie für gilt, wählen Sie die Option wie folgt aus:
 - Wenn Sie die Richtlinie auf alle Konten in Ihrer Organisation anwenden möchten, behalten Sie die Standardauswahl Alle Konten meiner AWS Organisation einbeziehen bei.
 - Wenn Sie die Richtlinie nur auf bestimmte Konten oder Konten in bestimmten AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Nur die angegebenen Konten und Organisationseinheiten einbeziehen aus und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie einbeziehen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

- Wenn Sie die Richtlinie für alle Konten oder Organisationseinheiten (OUs) außer einer bestimmten Gruppe von Konten oder AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Die angegebenen Konten und Organisationseinheiten ausschließen und alle anderen einbeziehen aus, und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie ausschließen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

Sie können nur eine der Optionen auswählen.

Nachdem Sie die Richtlinie angewendet haben, bewertet Firewall Manager automatisch alle neuen Konten anhand Ihrer Einstellungen. Wenn Sie beispielsweise nur bestimmte Konten angeben, wendet Firewall Manager die Richtlinie nicht auf neue Konten an. Ein weiteres Beispiel: Wenn Sie eine Organisationseinheit hinzufügen und der Organisationseinheit oder einer ihrer untergeordneten Organisationseinheiten ein Konto hinzufügen, wendet Firewall Manager die Richtlinie automatisch auf das neue Konto an.

11. Der Ressourcentyp für DNS-Firewall-Richtlinien ist VPC.
12. Wenn Sie unter Resources (Ressourcen) nur Ressourcen schützen (oder ausschließen) möchten, die bestimmte Tags haben, wählen Sie die entsprechende Option aus und geben Sie dann die Tags ein, die eingeschlossen oder ausgeschlossen werden sollen. Sie können nur eine Option auswählen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).

Wenn Sie mehrere Tags eingeben, muss eine Ressource über alle Tags verfügen, die eingeschlossen oder ausgeschlossen werden sollen.

13. Wählen Sie Weiter aus.
14. Fügen Sie für Policy-Tags alle Identifizierungs-Tags hinzu, die Sie für die Firewall Manager Manager-Richtlinie benötigen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).
15. Wählen Sie Weiter aus.
16. Überprüfen Sie die neue Richtlinie. Um Änderungen vorzunehmen, wählen Sie Edit (Bearbeiten) in dem Bereich, den Sie ändern möchten. Dadurch kehren Sie zum entsprechenden Schritt im Erstellungsassistenten zurück. Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen).

Eine AWS Firewall Manager Richtlinie für Palo Alto Networks Cloud NGFW erstellen

Mit einer Firewall Manager-Richtlinie für die Palo Alto Networks Cloud Next Generation Firewall (Palo Alto Networks Cloud NGFW) verwenden Sie Firewall Manager, um Palo Alto Networks Cloud NGFW-Ressourcen bereitzustellen und NGFW-Regelstapel zentral für all Ihre Konten zu verwalten. AWS

Informationen zu den Cloud NGFW-Richtlinien von Firewall Manager Palo Alto Networks finden Sie unter [NGFW-Richtlinien für die Cloud von Palo Alto Networks](#) Informationen zur Konfiguration und Verwaltung von Palo Alto Networks Cloud NGFW für Firewall Manager finden Sie in der Dokumentation [Palo Alto Networks Cloud NGFW von Palo Alto Networks](#). AWS

Voraussetzungen

Mehrere Schritte sind zur Vorbereitung Ihres Kontos auf AWS Firewall Manager zwingend erforderlich. Diese Schritte werden in [AWS Firewall Manager Voraussetzungen](#) beschrieben. Erfüllen Sie alle Voraussetzungen, bevor Sie mit dem nächsten Schritt fortfahren.

So erstellen Sie eine Firewall Manager Manager-Richtlinie für Palo Alto Networks Cloud NGFW (Konsole)

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie als Richtlinientyp Palo Alto Networks Cloud NGFW aus. Wenn Sie den Palo Alto Networks Cloud NGFW-Dienst noch nicht im AWS Marketplace abonniert haben, müssen Sie dies zuerst tun. Um im AWS Marketplace ein Abonnement abzuschließen, wählen Sie AWS Marketplace-Details anzeigen.
5. Wählen Sie als Bereitstellungsmodell entweder das verteilte Modell oder das zentralisierte Modell. Das Bereitstellungsmodell bestimmt, wie Firewall Manager Endpunkte für die Richtlinie verwaltet. Beim verteilten Modell verwaltet Firewall Manager Firewall-Endpunkte in jeder VPC,


die innerhalb des Richtlinienbereichs liegen. Mit dem zentralisierten Modell verwaltet Firewall Manager einen einzigen Endpunkt in einer Inspektions-VPC.

6. Wählen Sie für Region eine AWS-Region. Um Ressourcen in mehreren Regionen zu schützen, müssen Sie für jede Region separate Richtlinien erstellen.
7. Wählen Sie Weiter aus.
8. Geben Sie als Richtlinienname einen aussagekräftigen Namen ein.
9. Wählen Sie in der Richtlinienkonfiguration die Palo Alto Networks Cloud NGFW-Firewallrichtlinie aus, die dieser Richtlinie zugeordnet werden soll. Die Liste der Palo Alto Networks Cloud NGFW-Firewallrichtlinien enthält alle Palo Alto Networks Cloud NGFW-Firewallrichtlinien, die Ihrem Palo Alto Networks Cloud NGFW-Mandanten zugeordnet sind. Informationen zur Erstellung und Verwaltung von Palo Alto Networks Cloud NGFW-Firewallrichtlinien finden Sie im Abschnitt [Deploy Palo Alto Networks Cloud NGFW for](#) mit dem Thema im [Leitfaden Palo Alto Networks Cloud NGFW for Deployment](#). AWS AWS Firewall Manager AWS
10. Für die Palo Alto Networks Cloud NGFW-Protokollierung — optional — wählen Sie optional, welche Palo Alto Networks Cloud NGFW-Protokolltypen für Ihre Richtlinie protokolliert werden sollen. Informationen zu den NGFW-Protokolltypen in Palo Alto Networks Cloud finden [Sie unter Configure Logging for Palo Alto Networks Cloud NGFW on](#) im [Leitfaden Palo Alto Networks Cloud NGFW](#) for Deployment. AWS AWS

Geben Sie als Protokollziel an, wohin Firewall Manager Protokolle schreiben soll.

11. Wählen Sie Weiter aus.
12. Führen Sie unter Firewall-Endpunkt eines Drittanbieters konfigurieren einen der folgenden Schritte aus, je nachdem, ob Sie für die Erstellung Ihrer Firewall-Endpunkte das verteilte oder das zentralisierte Bereitstellungsmodell verwenden:
 - Wenn Sie das verteilte Bereitstellungsmodell für diese Richtlinie verwenden, wählen Sie unter Availability Zones aus, in welchen Availability Zones Firewall-Endpoints erstellt werden sollen. Sie können Availability Zones nach dem Namen der Availability Zone oder nach der Availability Zone ID auswählen.
 - Wenn Sie das zentralisierte Bereitstellungsmodell für diese Richtlinie verwenden, geben Sie in der AWS Firewall Manager Endpunktkonfiguration unter Inspektion-VPC-Konfiguration die AWS Konto-ID des Besitzers der Inspektion-VPC und die VPC-ID der Inspektion-VPC ein.
 - Wählen Sie unter Availability Zones aus, in welchen Availability Zones Firewall-Endpoints erstellt werden sollen. Sie können Availability Zones nach dem Namen der Availability Zone oder nach der Availability Zone ID auswählen.

13. Wenn Sie die CIDR-Blöcke für Firewall Manager zur Verwendung für Firewall-Subnetze in Ihren VPCs bereitstellen möchten, müssen sie alle /28 CIDR-Blöcke sein. Geben Sie einen Block pro Zeile ein. Wenn Sie diese weglassen, wählt Firewall Manager IP-Adressen für Sie aus den in den VPCs verfügbaren IP-Adressen aus.

 Note

Die automatische Korrektur erfolgt automatisch für AWS Firewall Manager Netzwerk-Firewall-Richtlinien, sodass Sie hier keine Option sehen, die auto Korrektur abzulehnen.

14. Wählen Sie Weiter aus.
15. Wählen Sie für den Geltungsbereich der Richtlinie unter „AWS-Konten Diese Richtlinie gilt für“ die Option wie folgt aus:
 - Wenn Sie die Richtlinie auf alle Konten in Ihrer Organisation anwenden möchten, behalten Sie die Standardauswahl Alle Konten meiner AWS Organisation einbeziehen bei.
 - Wenn Sie die Richtlinie nur auf bestimmte Konten oder Konten in bestimmten AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Nur die angegebenen Konten und Organisationseinheiten einbeziehen aus und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie einbeziehen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.
 - Wenn Sie die Richtlinie für alle Konten oder Organisationseinheiten (OUs) außer einer bestimmten Gruppe von Konten oder AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Die angegebenen Konten und Organisationseinheiten ausschließen und alle anderen einbeziehen aus, und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie ausschließen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

Sie können nur eine der Optionen auswählen.

Nachdem Sie die Richtlinie angewendet haben, bewertet Firewall Manager automatisch alle neuen Konten anhand Ihrer Einstellungen. Wenn Sie beispielsweise nur bestimmte Konten angeben, wendet Firewall Manager die Richtlinie nicht auf neue Konten an. Ein weiteres Beispiel:

Wenn Sie eine Organisationseinheit hinzufügen und der Organisationseinheit oder einer ihrer untergeordneten Organisationseinheiten ein Konto hinzufügen, wendet Firewall Manager die Richtlinie automatisch auf das neue Konto an.

16. Der Ressourcentyp für Netzwerk-Firewall-Richtlinien ist VPC.
17. Wenn Sie unter Resources (Ressourcen) nur Ressourcen schützen (oder ausschließen) möchten, die bestimmte Tags haben, wählen Sie die entsprechende Option aus und geben Sie dann die Tags ein, die eingeschlossen oder ausgeschlossen werden sollen. Sie können nur eine Option auswählen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).

Wenn Sie mehrere Tags eingeben, muss eine Ressource über alle Tags verfügen, die eingeschlossen oder ausgeschlossen werden sollen.

18. Wählen Sie für Kontenübergreifenden Zugriff gewähren die Option Vorlage herunterladen AWS CloudFormation aus. Dadurch wird eine AWS CloudFormation Vorlage heruntergeladen, mit der Sie einen AWS CloudFormation Stack erstellen können. Dieser Stack erstellt eine AWS Identity and Access Management Rolle, die Firewall Manager kontoübergreifende Berechtigungen zur Verwaltung von Palo Alto Networks Cloud NGFW-Ressourcen gewährt. Informationen zu Stacks finden Sie unter [Arbeiten mit Stacks](#) im Benutzerhandbuch.AWS CloudFormation
19. Wählen Sie Weiter aus.
20. Fügen Sie für Policy-Tags alle Identifizierungs-Tags hinzu, die Sie für die Firewall Manager Manager-Richtlinie benötigen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).
21. Wählen Sie Weiter aus.
22. Überprüfen Sie die neue Richtlinie. Um Änderungen vorzunehmen, wählen Sie Edit (Bearbeiten) in dem Bereich, den Sie ändern möchten. Dadurch kehren Sie zum entsprechenden Schritt im Erstellungsassistenten zurück. Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen).

Erstellen einer AWS Firewall Manager Richtlinie für Fortigate Cloud Native Firewall (CNF) as a Service

Mit einer Firewall Manager-Richtlinie für Fortigate CNF können Sie den Firewall Manager verwenden, um Fortigate CNF-Ressourcen für all Ihre Konten bereitzustellen und zu verwalten. AWS

Informationen zu den Fortigate CNF-Richtlinien von Firewall Manager finden Sie unter. [Richtlinien für die Fortigate Cloud Native Firewall \(CNF\) als Service](#) [Informationen zur Konfiguration von Fortigate CNF für die Verwendung mit Firewall Manager finden Sie in der Fortinet-Dokumentation.](#)

Voraussetzungen

Mehrere Schritte sind zur Vorbereitung Ihres Kontos auf AWS Firewall Manager zwingend erforderlich. Diese Schritte werden in [AWS Firewall Manager Voraussetzungen](#) beschrieben. Erfüllen Sie alle Voraussetzungen, bevor Sie mit dem nächsten Schritt fortfahren.

So erstellen Sie eine Firewall Manager Manager-Richtlinie für Fortigate CNF (Konsole)

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).


Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie als Richtlinientyp Fortigate Cloud Native Firewall (CNF) as a Service aus. Wenn Sie den [Fortigate CNF-Service im AWS Marketplace](#) noch nicht abonniert haben, müssen Sie dies zuerst tun. Um im AWS Marketplace ein Abonnement abzuschließen, wählen Sie AWS Marketplace-Details anzeigen.
5. Wählen Sie als Bereitstellungsmodell entweder das verteilte Modell oder das zentralisierte Modell. Das Bereitstellungsmodell bestimmt, wie Firewall Manager Endpunkte für die Richtlinie verwaltet. Beim verteilten Modell verwaltet Firewall Manager Firewall-Endpunkte in jeder VPC, die innerhalb des Richtlinienbereichs liegen. Mit dem zentralisierten Modell verwaltet Firewall Manager einen einzigen Endpunkt in einer Inspektions-VPC.
6. Wählen Sie für Region eine AWS-Region. Um Ressourcen in mehreren Regionen zu schützen, müssen Sie für jede Region separate Richtlinien erstellen.
7. Wählen Sie Weiter aus.
8. Geben Sie als Richtliniennamen einen aussagekräftigen Namen ein.
9. Wählen Sie in der Richtlinienkonfiguration die Fortigate CNF-Firewall-Richtlinie aus, die dieser Richtlinie zugeordnet werden soll. Die Liste der Fortigate CNF-Firewallrichtlinien enthält alle Fortigate CNF-Firewallrichtlinien, die Ihrem Fortigate CNF-Mandanten zugeordnet sind.

[Informationen zur Erstellung und Verwaltung von Fortigate CNF-Mandanten finden Sie in der Fortinet-Dokumentation.](#)

10. Wählen Sie Weiter aus.
11. Führen Sie unter Firewall-Endpunkt eines Drittanbieters konfigurieren einen der folgenden Schritte aus, je nachdem, ob Sie für die Erstellung Ihrer Firewall-Endpunkte das verteilte oder das zentralisierte Bereitstellungsmodell verwenden:
 - Wenn Sie das verteilte Bereitstellungsmodell für diese Richtlinie verwenden, wählen Sie unter Availability Zones aus, in welchen Availability Zones Firewall-Endpoints erstellt werden sollen. Sie können Availability Zones nach dem Namen der Availability Zone oder nach der Availability Zone ID auswählen.
 - Wenn Sie das zentralisierte Bereitstellungsmodell für diese Richtlinie verwenden, geben Sie in der AWS Firewall Manager Endpunktkonfiguration unter Inspektion-VPC-Konfiguration die AWS Konto-ID des Besitzers der Inspektion-VPC und die VPC-ID der Inspektion-VPC ein.
 - Wählen Sie unter Availability Zones aus, in welchen Availability Zones Firewall-Endpoints erstellt werden sollen. Sie können Availability Zones nach dem Namen der Availability Zone oder nach der Availability Zone ID auswählen.
12. Wenn Sie die CIDR-Blöcke für Firewall Manager zur Verwendung für Firewall-Subnetze in Ihren VPCs bereitstellen möchten, müssen sie alle /28 CIDR-Blöcke sein. Geben Sie einen Block pro Zeile ein. Wenn Sie diese weglassen, wählt Firewall Manager IP-Adressen für Sie aus den in den VPCs verfügbaren IP-Adressen aus.

 Note

Die automatische Korrektur erfolgt automatisch für AWS Firewall Manager Netzwerk-Firewall-Richtlinien, sodass Sie hier keine Option sehen, die auto Korrektur abzulehnen.

13. Wählen Sie Weiter aus.
14. Wählen Sie für den Geltungsbereich der Richtlinie unter „AWS-Konten Diese Richtlinie gilt für“ die Option wie folgt aus:
 - Wenn Sie die Richtlinie auf alle Konten in Ihrer Organisation anwenden möchten, behalten Sie die Standardauswahl Alle Konten meiner AWS Organisation einbeziehen bei.
 - Wenn Sie die Richtlinie nur auf bestimmte Konten oder Konten in bestimmten AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Nur die angegebenen Konten und Organisationseinheiten einbeziehen aus und fügen Sie dann

die Konten und Organisationseinheiten hinzu, die Sie einbeziehen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

- Wenn Sie die Richtlinie für alle Konten oder Organisationseinheiten (OUs) außer einer bestimmten Gruppe von Konten oder AWS Organizations Organisationseinheiten (OUs) anwenden möchten, wählen Sie Die angegebenen Konten und Organisationseinheiten ausschließen und alle anderen einbeziehen aus, und fügen Sie dann die Konten und Organisationseinheiten hinzu, die Sie ausschließen möchten. Die Angabe einer OU ist gleichwertig mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

Sie können nur eine der Optionen auswählen.

Nachdem Sie die Richtlinie angewendet haben, bewertet Firewall Manager automatisch alle neuen Konten anhand Ihrer Einstellungen. Wenn Sie beispielsweise nur bestimmte Konten angeben, wendet Firewall Manager die Richtlinie nicht auf neue Konten an. Ein weiteres Beispiel: Wenn Sie eine Organisationseinheit hinzufügen und der Organisationseinheit oder einer ihrer untergeordneten Organisationseinheiten ein Konto hinzufügen, wendet Firewall Manager die Richtlinie automatisch auf das neue Konto an.

15. Der Ressourcentyp für Netzwerk-Firewall-Richtlinien ist VPC.
16. Wenn Sie unter Resources (Ressourcen) nur Ressourcen schützen (oder ausschließen) möchten, die bestimmte Tags haben, wählen Sie die entsprechende Option aus und geben Sie dann die Tags ein, die eingeschlossen oder ausgeschlossen werden sollen. Sie können nur eine Option auswählen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).

Wenn Sie mehrere Tags eingeben, muss eine Ressource über alle Tags verfügen, die eingeschlossen oder ausgeschlossen werden sollen.

17. Wählen Sie für Kontenübergreifenden Zugriff gewähren die Option Vorlage herunterladen AWS CloudFormation aus. Dadurch wird eine AWS CloudFormation Vorlage heruntergeladen, mit der Sie einen AWS CloudFormation Stack erstellen können. Dieser Stack erstellt eine AWS Identity and Access Management Rolle, die Firewall Manager kontoübergreifende Berechtigungen zur Verwaltung von Fortigate CNF-Ressourcen gewährt. Informationen zu Stacks finden Sie unter [Arbeiten mit Stacks](#) im Benutzerhandbuch.AWS CloudFormation Um einen Stack zu erstellen, benötigen Sie die Konto-ID aus dem Fortigate CNF-Portal.

18. Wählen Sie Weiter aus.
19. Fügen Sie für Policy-Tags alle Identifizierungs-Tags hinzu, die Sie für die Firewall Manager Manager-Richtlinie benötigen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).
20. Wählen Sie Weiter aus.
21. Überprüfen Sie die neue Richtlinie. Um Änderungen vorzunehmen, wählen Sie Edit (Bearbeiten) in dem Bereich, den Sie ändern möchten. Dadurch kehren Sie zum entsprechenden Schritt im Erstellungsassistenten zurück. Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen).

Löschen einer AWS Firewall Manager Richtlinie

Sie können eine Firewall Manager-Richtlinie durch Ausführen der folgenden Schritte löschen.

So löschen Sie eine Richtlinie (Konsole)

1. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
2. Wählen Sie die Option neben der Richtlinie aus, die Sie löschen möchten.
3. Wählen Sie Löschen aus.

Note

Wenn Sie eine allgemeine Sicherheitsgruppenrichtlinie von Firewall Manager löschen, um die replizierten Sicherheitsgruppen der Richtlinie zu entfernen, wählen Sie die Option zum Bereinigen der durch die Richtlinie erstellten Ressourcen. Andernfalls bleiben die Replikate nach dem Löschen der Primärdatei erhalten und müssen in jeder Amazon VPC-Instance manuell verwaltet werden.

Important

Wenn Sie eine Firewall Manager Shield Advanced-Richtlinie löschen, wird die Richtlinie gelöscht, aber Ihre Konten haben weiterhin Shield Advanced abonniert.

AWS Firewall Manager Geltungsbereich der Politik

Der Geltungsbereich der Richtlinie definiert, wo die Richtlinie gilt. Sie können entweder zentral gesteuerte Richtlinien auf alle Ihre Konten und Ressourcen innerhalb Ihrer Organisation oder auf eine Teilmenge Ihrer Konten und Ressourcen anwenden. AWS Organizations Anweisungen zur Festlegung des Geltungsbereichs von Richtlinien finden Sie unter [Eine AWS Firewall Manager Richtlinie erstellen](#).

Optionen für den Geltungsbereich der Richtlinie in AWS Firewall Manager

Wenn Sie Ihrer Organisation ein neues Konto oder eine neue Ressource hinzufügen, bewertet Firewall Manager es automatisch anhand Ihrer Einstellungen für jede Richtlinie und wendet die Richtlinie auf der Grundlage dieser Einstellungen an. Sie können beispielsweise festlegen, dass eine Richtlinie auf alle Konten mit Ausnahme der Kontonummern in einer bestimmten Liste angewendet wird. Sie können auch festlegen, dass eine Richtlinie nur auf Ressourcen angewendet wird, die alle Tags in einer Liste enthalten.

AWS-Konten im Geltungsbereich

Die Einstellungen, die Sie angeben, um die von der Richtlinie AWS-Konten betroffenen Personen zu definieren, bestimmen, auf welche der Konten in Ihrer AWS Organisation die Richtlinie angewendet werden soll. Sie können die Richtlinie auf eine der folgenden Arten anwenden:

- Auf alle Konten in Ihrer Organisation
- Nur auf eine bestimmte Liste eingeschlossener Kontonummern und AWS Organizations - Organisationseinheiten (OUs)
- Auf alle Kontonummern und Organisationseinheiten außer einer bestimmten Liste ausgeschlossener Kontonummern und AWS Organizations -Organisationseinheiten (OUs)

Informationen dazu AWS Organizations finden Sie im [AWS Organizations Benutzerhandbuch](#).

Ressourcen im Geltungsbereich

Ähnlich wie bei den Einstellungen für Konten im Geltungsbereich bestimmen die Einstellungen, die Sie für Ressourcen angeben, auf welche Ressourcentypen im Geltungsbereich die Richtlinie angewendet werden soll. Sie können eine der folgenden Optionen auswählen:

- Alle Ressourcen
- Ressourcen, die alle von Ihnen angegebenen Tags enthalten

- Alle Ressourcen außer denen, die alle von Ihnen angegebenen Tags enthalten

Weitere Informationen zum Kennzeichnen Ihrer Ressourcen finden Sie unter [Arbeiten mit Tag-Editor](#).

Verwaltung des Richtlinienumfangs in AWS Firewall Manager

Sobald Richtlinien eingerichtet sind, verwaltet Firewall Manager sie kontinuierlich und wendet sie entsprechend dem Geltungsbereich der Richtlinie auf neue AWS-Konten Ressourcen an, sobald sie hinzugefügt werden.

Verwaltung AWS-Konten und Ressourcen durch Firewall Manager

Wenn ein Konto oder eine Ressource aus irgendeinem Grund den Geltungsbereich verlässt, AWS Firewall Manager werden Schutzmaßnahmen nicht automatisch entfernt oder von Firewall Manager verwaltete Ressourcen gelöscht, es sei denn, Sie aktivieren das Kontrollkästchen Schutz automatisch von Ressourcen entfernen, die den Geltungsbereich der Richtlinie verlassen.

Note

Die Option Automatisch den Schutz von Ressourcen entfernen, die den Geltungsbereich der Richtlinie verlassen, ist für Richtlinien oder Classic nicht verfügbar. AWS Shield Advanced AWS WAF

Wenn Sie dieses Kontrollkästchen aktivieren, werden AWS Firewall Manager die Ressourcen, die Firewall Manager für Konten verwaltet, automatisch bereinigt, wenn diese Konten den Richtlinienbereich verlassen. Beispielsweise trennt Firewall Manager die Zuordnung einer von Firewall Manager verwalteten Web-ACL zu einer geschützten Kundenressource, wenn die Kundenressource den Geltungsbereich der Richtlinie verlässt.

Um zu bestimmen, welche Ressourcen aus dem Schutz entfernt werden sollen, wenn eine Kundenressource den Richtlinienbereich verlässt, befolgt Firewall Manager die folgenden Richtlinien:

- Standardverhalten:
 - Die zugehörigen AWS Config verwalteten Regeln werden gelöscht. Dieses Verhalten ist unabhängig vom Kontrollkästchen.
 - Alle zugehörigen AWS WAF Web Access Control Lists (Web-ACLs), die keine Ressourcen enthalten, werden gelöscht. Dieses Verhalten ist unabhängig vom Kontrollkästchen.

- Jede geschützte Ressource, die den Gültigkeitsbereich überschreitet, bleibt zugeordnet und geschützt. Beispielsweise bleibt ein Application Load Balancer oder eine API von API Gateway, die mit einer Web-ACL verknüpft ist, mit der Web-ACL verknüpft, und der Schutz bleibt bestehen.
- Wenn das Kontrollkästchen Schutz von Ressourcen, die den Geltungsbereich der Richtlinie verlassen, automatisch entfernen aktiviert ist:
 - Die zugehörigen AWS Config verwalteten Regeln werden gelöscht. Dieses Verhalten ist unabhängig vom Kontrollkästchen.
 - Alle zugehörigen AWS WAF Web Access Control Lists (Web-ACLs), die keine Ressourcen enthalten, werden gelöscht. Dieses Verhalten ist unabhängig vom Kontrollkästchen.
 - Jede geschützte Ressource, die den Geltungsbereich verlässt, wird automatisch getrennt und aus dem Schutz entfernt, wenn sie den Richtlinienbereich verlässt. Beispielsweise wird eine Elastic Inference Accelerator- oder Amazon EC2 EC2-Instance automatisch von der replizierten Sicherheitsgruppe getrennt, wenn sie den Richtlinienbereich verlässt. Die replizierte Sicherheitsgruppe und ihre Ressourcen werden automatisch aus dem Schutz entfernt.

Verwaltete Listen

Verwaltete Anwendungs- und Protokolllisten optimieren Ihre Konfiguration und Verwaltung von Sicherheitsgruppenrichtlinien für AWS Firewall Manager Content Audits. Mithilfe verwalteter Listen definieren Sie die Protokolle und Anwendungen, die Ihre Richtlinie zulässt und welche nicht. Informationen zu Sicherheitsgruppenrichtlinien für Content Audits finden Sie unter [Inhaltsprüfungssicherheitsgruppenrichtlinien](#).

Sie können die folgenden Typen von verwalteten Listen in einer Sicherheitsgruppenrichtlinie für die Inhaltsüberwachung verwenden:

- Anwendungslisten und Protokolllisten von Firewall Manager — Firewall Manager verwaltet diese Listen.
 - Die Anwendungslisten enthalten `FMS-Default-Public-Access-Apps-Allowed` und `FMS-Default-Public-Access-Apps-Denied`, in denen häufig verwendete Anwendungen beschrieben werden, die der Öffentlichkeit erlaubt oder verweigert werden sollten.
 - Die Protokolllisten enthalten `FMS-Default-Protocols-Allowed` eine Liste häufig verwendeter Protokolle, die der Öffentlichkeit zugänglich sein sollten. Sie können jede Liste verwenden, die Firewall Manager verwaltet, aber Sie können sie nicht bearbeiten oder löschen.

- Benutzerdefinierte Anwendungslisten und Protokolllisten — Sie verwalten diese Listen. Sie können Listen beider Typen mit den Einstellungen erstellen, die Sie benötigen. Sie haben die volle Kontrolle über Ihre eigenen benutzerdefinierten verwalteten Listen und können sie nach Bedarf erstellen, bearbeiten und löschen.

Note

Derzeit überprüft Firewall Manager keine Verweise auf eine benutzerdefinierte verwaltete Liste, wenn Sie sie löschen. Das bedeutet, dass Sie eine benutzerdefinierte Liste verwalteter Anwendungen oder Protokolle löschen können, selbst wenn sie von einer aktiven Richtlinie verwendet wird. Dies kann dazu führen, dass die Richtlinie nicht mehr funktioniert. Löschen Sie eine Anwendungs- oder Protokollliste erst, nachdem Sie sich vergewissert haben, dass keine aktiven Richtlinien darauf verweisen.

Verwaltete Listen sind AWS Ressourcen. Sie können eine benutzerdefinierte verwaltete Liste taggen. Sie können eine verwaltete Liste von Firewall Manager nicht taggen.

Versionierung verwalteter Listen

Für benutzerdefinierte verwaltete Listen gibt es keine Versionen. Wenn Sie eine benutzerdefinierte Liste bearbeiten, verwenden Richtlinien, die auf die Liste verweisen, automatisch die aktualisierte Liste.

Von Firewall Manager verwaltete Listen sind versioniert. Das Firewall Manager Manager-Serviceteam veröffentlicht bei Bedarf neue Versionen, um die Listen mit den besten Sicherheitspraktiken zu versehen.

Wenn Sie eine von Firewall Manager verwaltete Liste in einer Richtlinie verwenden, wählen Sie Ihre Versionsstrategie wie folgt aus:

- Letzte verfügbare Version — Wenn Sie keine explizite Versionseinstellung für die Liste angeben, verwendet Ihre Richtlinie automatisch die neueste Version. Dies ist die einzige Option, die über die Konsole verfügbar ist.
- Explizite Version — Wenn Sie eine Version für die Liste angeben, verwendet Ihre Richtlinie diese Version. Ihre Richtlinie bleibt an die von Ihnen angegebene Version gebunden, bis Sie die Versionseinstellung ändern. Um die Version anzugeben, müssen Sie die Richtlinie außerhalb der Konsole definieren, z. B. über die CLI oder eines der SDKs.

Weitere Informationen zur Auswahl der Versionseinstellung für eine Liste finden Sie unter [Verwenden verwalteter Listen in Ihren Sicherheitsgruppenrichtlinien für die Inhaltsüberwachung](#).

Verwenden verwalteter Listen in Ihren Sicherheitsgruppenrichtlinien für die Inhaltsüberwachung

Wenn Sie eine Gruppenrichtlinie für die Inhaltsüberwachung erstellen, können Sie festlegen, ob Sie Regeln für verwaltete Überwachungsrichtlinien verwenden möchten. Einige Einstellungen für diese Option erfordern eine Liste verwalteter Anwendungen oder Protokolle. Zu diesen Einstellungen gehören beispielsweise Protokolle, die in Sicherheitsgruppenregeln zulässig sind, und Anwendungen können auf das Internet zugreifen.

Die folgenden Einschränkungen gelten für jede Richtlinieneinstellung, die eine verwaltete Liste verwendet:


- Sie können für jede Einstellung höchstens eine von Firewall Manager verwaltete Liste angeben. Standardmäßig können Sie höchstens eine benutzerdefinierte Liste angeben. Das Limit für benutzerdefinierte Listen ist ein unverbindliches Kontingent, sodass Sie eine Erhöhung beantragen können. Weitere Informationen finden Sie unter [AWS Firewall Manager Kontingente](#).
- Wenn Sie in der Konsole eine von Firewall Manager verwaltete Liste auswählen, können Sie die Version nicht angeben. Die Richtlinie verwendet immer die neueste Version der Liste. Um die Version anzugeben, müssen Sie die Richtlinie außerhalb der Konsole definieren, z. B. über die CLI oder eines der SDKs. Informationen zur Versionsverwaltung für verwaltete Listen mit Firewall Manager finden Sie unter [Versionierung verwalteter Listen](#).

Informationen zum Erstellen einer Sicherheitsgruppenrichtlinie für die Inhaltsüberwachung über die Konsole finden Sie unter [Erstellen einer Inhaltsprüfungssicherheitsgruppenrichtlinie](#).

Eine benutzerdefinierte Liste verwalteter Anwendungen erstellen

Um eine benutzerdefinierte Liste verwalteter Anwendungen zu erstellen

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

 Note


Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Anwendungslisten aus.
3. Wählen Sie auf der Seite Anwendungslisten die Option Anwendungsliste erstellen aus.
4. Geben Sie auf der Seite Anwendungsliste erstellen Ihrer Liste einen Namen. Verwenden Sie das Präfix nicht, fms - da es für Firewall Manager reserviert ist.
5. Geben Sie eine Anwendung an, indem Sie entweder das Protokoll und die Portnummer angeben oder indem Sie eine Anwendung aus der Dropdownliste Typ auswählen. Geben Sie Ihrer Anwendungsspezifikation einen Namen.
6. Wählen Sie Nach Bedarf weitere hinzufügen und geben Sie die Anwendungsinformationen ein, bis Sie Ihre Liste abgeschlossen haben.
7. (Optional) Fügen Sie Ihrer Liste Stichwörter hinzu.
8. Wählen Sie Speichern, um Ihre Liste zu speichern und zur Seite mit den Anwendungslisten zurückzukehren.

Eine benutzerdefinierte Liste verwalteter Protokolle erstellen

Um eine benutzerdefinierte Liste verwalteter Protokolle zu erstellen

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

 Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Protokolllisten aus.
3. Wählen Sie auf der Seite Protokolllisten die Option Protokollliste erstellen aus.

4. Geben Sie auf der Seite zur Erstellung der Protokollliste Ihrer Liste einen Namen. Verwenden Sie das Präfix nicht, fms- da es für Firewall Manager reserviert ist.
5. Geben Sie ein Protokoll an.
6. Wählen Sie Nach Bedarf weitere hinzufügen und geben Sie die Protokollinformationen ein, bis Sie Ihre Liste abgeschlossen haben.
7. (Optional) Fügen Sie Ihrer Liste Stichwörter hinzu.
8. Wählen Sie Speichern, um Ihre Liste zu speichern und zur Seite mit den Protokolllisten zurückzukehren.

Eine verwaltete Liste anzeigen

Um eine Anwendungs- oder Protokollliste anzuzeigen

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Anwendungslisten oder Protokolllisten aus.

Auf der Seite werden alle Listen des ausgewählten Typs angezeigt, die für Sie verfügbar sind. Die von Firewall Manager verwalteten Listen haben ein Y in der ManagedListSpalte.

3. Um die Details einer Liste zu sehen, wählen Sie ihren Namen. Auf der Detailseite werden der Inhalt der Liste und alle Tags angezeigt.

Für verwaltete Listen mit Firewall Manager können Sie die verfügbaren Versionen auch anzeigen, indem Sie das Drop-down-Menü Version auswählen.

Löschen einer benutzerdefinierten verwalteten Liste

Sie können benutzerdefinierte verwaltete Listen löschen. Sie können die von Firewall Manager verwalteten Listen nicht bearbeiten oder löschen.

Note

Derzeit überprüft Firewall Manager keine Verweise auf eine benutzerdefinierte verwaltete Liste, wenn Sie sie löschen. Das bedeutet, dass Sie eine benutzerdefinierte Liste verwalteter Anwendungen oder Protokolle löschen können, selbst wenn sie von einer aktiven Richtlinie verwendet wird. Dies kann dazu führen, dass die Richtlinie nicht mehr funktioniert. Löschen Sie eine Anwendungs- oder Protokollliste erst, wenn Sie sich vergewissert haben, dass keine aktiven Richtlinien darauf verweisen.

Um eine benutzerdefinierte verwaltete Anwendungs- oder Protokollliste zu löschen

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Stellen Sie sicher, dass die Liste, die Sie löschen möchten, in keiner Ihrer Gruppenrichtlinien für Auditsicherheit verwendet wird, indem Sie wie folgt vorgehen:
 - a. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
 - b. Wählen und bearbeiten Sie auf der AWS Firewall Manager Richtlinienseite Ihre Auditsicherheitsgruppen und entfernen Sie alle Verweise auf die benutzerdefinierte Liste, die Sie löschen möchten.

Wenn Sie eine benutzerdefinierte verwaltete Liste löschen, die in einer Gruppenrichtlinie für Überwachungssicherheit verwendet wird, funktioniert die Richtlinie, die sie verwendet, möglicherweise nicht mehr.

3. Wählen Sie im Navigationsbereich je nach Art der Liste, die Sie löschen möchten, Anwendungslisten oder Protokolllisten aus.
4. Wählen Sie auf der Listenseite die benutzerdefinierte Liste aus, die Sie löschen möchten, und klicken Sie auf Löschen.

AWS WAF Richtlinien

In einer Firewall Manager AWS WAF Manager-Richtlinie geben Sie die AWS WAF Regelgruppen an, die Sie für Ihre Ressourcen verwenden möchten. Wenn Sie die Richtlinie anwenden, erstellt Firewall Manager Web-ACLs in Konten innerhalb des Richtlinienbereichs, je nachdem, wie Sie die Verwaltung von Web-ACLs in Ihrer Richtlinie konfigurieren. In den durch die Richtlinie erstellten Web-ACLs können einzelne Kontomanager zusätzlich zu den Regelgruppen, die Sie mit Firewall Manager definiert haben, Regeln und Regelgruppen hinzufügen.

So verwaltet Firewall Manager Web-ACLs

Firewall Manager erstellt Web-ACLs auf der Grundlage der Konfiguration der Einstellung Nicht zugeordnete Web-ACLs verwalten in Ihrer Richtlinie oder der `optimizeUnassociatedWebACL` Einstellung für den [SecurityServicePolicyData](#) Datentyp in der API.

Wenn Sie die Verwaltung nicht zugeordneter Web-ACLs aktivieren, erstellt Firewall Manager Web-ACLs in den Konten innerhalb des Richtlinienbereichs nur, wenn die Web-ACLs von mindestens einer Ressource verwendet werden. Wenn ein Konto zu irgendeinem Zeitpunkt in den Geltungsbereich der Richtlinie fällt, erstellt Firewall Manager automatisch eine Web-ACL in dem Konto, sofern mindestens eine Ressource die Web-ACL verwendet. Wenn Sie die Verwaltung nicht verknüpfter Web-ACLs aktivieren, führt Firewall Manager eine einmalige Bereinigung der nicht verknüpften Web-ACLs in Ihrem Konto durch. Während der Bereinigung überspringt Firewall Manager alle Web-ACLs, die Sie nach ihrer Erstellung geändert haben, z. B. wenn Sie der Web-ACL eine Regelgruppe hinzugefügt oder deren Einstellungen geändert haben. Der Bereinigungsprozess kann mehrere Stunden dauern. Wenn eine Ressource den Richtlinienbereich verlässt, nachdem Firewall Manager eine Web-ACL erstellt hat, trennt Firewall Manager die Zuordnung der Ressource von der Web-ACL, bereinigt aber nicht die nicht zugeordnete Web-ACL. Firewall Manager bereinigt nicht verknüpfte Web-ACLs nur, wenn Sie die Verwaltung nicht verknüpfter Web-ACLs in einer Richtlinie zum ersten Mal aktivieren.

Wenn Sie diese Option nicht aktivieren, verwaltet Firewall Manager keine nicht verknüpften Web-ACLs, und Firewall Manager erstellt automatisch eine Web-ACL für jedes Konto, das innerhalb des Richtlinienbereichs liegt.

Stichproben und Metriken CloudWatch

AWS Firewall Manager aktiviert Stichproben und CloudWatch Amazon-Metriken für die Web-ACLs und Regelgruppen, die es für eine AWS WAF Richtlinie erstellt.

Benennungsstruktur für Web-ACLs

Wenn Firewall Manager eine Web-ACL für die Richtlinie erstellt, benennt er die Web-ACLFMMangedWebACLV2-*policy name-timestamp*. Der Zeitstempel wird in UTC-Millisekunden angegeben. z. B. FMMangedWebACLV2-MyWAFPolicyName-1621880374078.

Note

Wenn eine mit [erweiterter automatischer DDoS-Abwehr auf Anwendungsebene](#) konfigurierte Ressource in den Geltungsbereich einer AWS WAF Richtlinie fällt, kann Firewall Manager die durch die AWS WAF Richtlinie erstellte Web-ACL der Ressource nicht zuordnen.

Regelgruppen in Richtlinien AWS WAF

Die Web-ACLs, die durch Firewall Manager AWS WAF Manager-Richtlinien verwaltet werden, enthalten drei Regelsätze. Diese Sätze bieten eine höhere Priorisierung für die Regeln und Regelgruppen in der Web-ACL:

- Erste Regelgruppen, von Ihnen in der Firewall Manager AWS WAF Manager-Richtlinie definiert. AWS WAF wertet diese Regelgruppen zuerst aus.
- Regeln und Regelgruppen, die von den Kontomanagern in den Web-ACLs definiert werden. AWS WAF wertet als nächstes alle kontoverwalteten Regeln oder Regelgruppen aus.
- Letzte Regelgruppen, von Ihnen in der Firewall Manager AWS WAF Manager-Richtlinie definiert. AWS WAF wertet diese Regelgruppen zuletzt aus.

In jedem dieser Regelsätze werden Regeln und Regelgruppen wie üblich anhand ihrer Prioritätseinstellungen innerhalb des Satzes AWS WAF ausgewertet.

In dem ersten und letzten Regelgruppensatz der Richtlinie können Sie nur Regelgruppen hinzufügen. Sie können verwaltete Regelgruppen verwenden, die von AWS Managed Rules und AWS Marketplace Verkäufern für Sie erstellt und verwaltet werden. Sie können auch eigene Regelgruppen verwalten und verwenden. Weitere Informationen über alle diese Aktionen finden Sie unter [Regelgruppen](#).

Wenn Sie Ihre eigenen Regelgruppen verwenden möchten, erstellen Sie diese, bevor Sie Ihre Firewall Manager AWS WAF Manager-Richtlinie erstellen. Anleitungen finden Sie unter [Verwaltung Ihrer eigenen Regelgruppen](#). Um eine einzelne benutzerdefinierte Regel verwenden zu können, müssen Sie eine eigene Regelgruppe definieren, Ihre Regel darin definieren und dann die Regelgruppe in der Richtlinie verwenden.

Die ersten und letzten AWS WAF Regelgruppen, die Sie über Firewall Manager verwalten, haben Namen `POSTFMManged-`, die mit dem `PREFMManged-` Namen der Firewall Manager Manager-Richtlinie und dem Zeitstempel für die Erstellung der Regelgruppe in UTC-Millisekunden beginnen bzw. darauf folgen. z. B. `PREFMManged-MyWAFPolicyName-1621880555123`.

Informationen darüber, wie Webanfragen AWS WAF ausgewertet werden, finden Sie unter

[Auswertung von Web-ACL-Regeln und -Regelgruppen](#)

Informationen zum Erstellen einer Firewall Manager AWS WAF Manager-Richtlinie finden Sie unter [Eine AWS Firewall Manager Richtlinie erstellen für AWS WAF](#).

Firewall Manager ermöglicht Sampling und CloudWatch Amazon-Metriken für die Regelgruppen, die Sie für die AWS WAF Richtlinie definieren.

Einzelne Kontoinhaber haben die vollständige Kontrolle über die Metriken und die Sampling-Konfiguration für jede Regel oder Regelgruppe, die sie zu den verwalteten Web-ACLs der Richtlinie hinzufügen.

Konfiguration der Protokollierung für eine Richtlinie AWS WAF

Sie können die zentrale Protokollierung für Ihre AWS WAF Richtlinien aktivieren, um detaillierte Informationen über den Datenverkehr zu erhalten, der von Ihrer Web-ACL innerhalb Ihres Unternehmens analysiert wird. Zu den Informationen in den Protokollen gehören der Zeitpunkt, zu dem die Anfrage von Ihrer AWS Ressource AWS WAF eingegangen ist, detaillierte Informationen zu der Anfrage und die Aktion für die Regel, der jede Anfrage von allen im Geltungsbereich befindlichen Konten entsprach. Sie können Ihre Protokolle an einen Amazon Data Firehose-Datenstream oder einen Amazon Simple Storage Service (S3) -Bucket senden. Informationen zur AWS WAF Protokollierung finden Sie [AWS WAF Web-ACL-Verkehr protokollieren](#) im AWS WAF Entwicklerhandbuch.

Note

AWS Firewall Manager unterstützt diese Option für AWS WAFV2, nicht für AWS WAF Classic.

Themen

- [Ziele protokollieren](#)
- [Aktivieren der Protokollierung](#)

- [Deaktivieren der Protokollierung](#)

Ziele protokollieren

In diesem Abschnitt werden die Protokollierungsziele beschrieben, an die Sie Ihre AWS WAF Richtlinienprotokolle senden können. Jeder Abschnitt enthält Anleitungen zum Konfigurieren der Protokollierung für den Zieltyp und Informationen zu jedem Verhalten, das für den jeweiligen Zieltyp spezifisch ist. Nachdem Sie Ihr Protokollierungsziel konfiguriert haben, können Sie dessen Spezifikationen für Ihre Firewall Manager AWS WAF Manager-Richtlinie angeben, um mit der Protokollierung zu beginnen.

Firewall Manager hat nach der Erstellung der Protokollierungskonfiguration keinen Einblick in Protokollfehler. Es liegt in Ihrer Verantwortung, zu überprüfen, ob die Protokollzustellung wie gewünscht funktioniert.

Note

Firewall Manager ändert keine vorhandenen Protokollierungskonfigurationen in den Mitgliedskonten Ihrer Organisation.

Themen

- [Amazon Data Firehose-Datenströme](#)
- [Amazon-Simple-Storage-Service-Buckets](#)

Amazon Data Firehose-Datenströme

Dieses Thema enthält Informationen zum Senden Ihrer Web-ACL-Traffic-Logs an einen Amazon Data Firehose-Datenstream.

Wenn Sie die Amazon Data Firehose-Protokollierung aktivieren, sendet Firewall Manager Protokolle von den Web-ACLs Ihrer Richtlinie an eine Amazon Data Firehose, für die Sie ein Speicherziel konfiguriert haben. Nachdem Sie die Protokollierung aktiviert haben AWS WAF , werden Protokolle für jede konfigurierte Web-ACL über den HTTPS-Endpunkt von Kinesis Data Firehose an das konfigurierte Speicherziel gesendet. Bevor Sie ihn verwenden, testen Sie Ihren Lieferstream, um sicherzustellen, dass er über einen ausreichenden Durchsatz verfügt, um die Logs Ihres Unternehmens zu verarbeiten. Weitere Informationen zum Erstellen einer Amazon Kinesis Data

Firehose und zum Überprüfen der gespeicherten Protokolle finden Sie unter [Was ist Amazon Data Firehose?](#)

Sie benötigen die folgenden Berechtigungen, um die Protokollierung mit einer Kinesis erfolgreich zu aktivieren:

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

Wenn Sie ein Amazon Data Firehose-Protokollierungsziel für eine AWS WAF Richtlinie konfigurieren, erstellt Firewall Manager eine Web-ACL für die Richtlinie im Firewall Manager Manager-Administratorkonto wie folgt:

- Firewall Manager erstellt die Web-ACL im Firewall Manager Manager-Administratorkonto, unabhängig davon, ob das Konto in den Geltungsbereich der Richtlinie fällt.
- Für die Web-ACL ist die Protokollierung mit einem Protokollnamen aktiviert `FMMangedWebACLV2-Logging` *policy name-timestamp*, wobei der Zeitstempel die UTC-Zeit in Millisekunden angibt, zu der das Protokoll für die Web-ACL aktiviert wurde. z. B. `FMMangedWebACLV2-LoggingMyWAFPolicyName-1621880565180`. Die Web-ACL hat keine Regelgruppen und keine zugehörigen Ressourcen.
- Die Web-ACL wird Ihnen gemäß den AWS WAF Preisrichtlinien in Rechnung gestellt. Weitere Informationen finden Sie unter [AWS WAF -Preisgestaltung](#).
- Firewall Manager löscht die Web-ACL, wenn Sie die Richtlinie löschen.

Weitere Informationen zu serviceverknüpften Rollen und zur `iam:CreateServiceLinkedRole`-Berechtigung finden Sie unter [Verwenden von serviceverknüpften Rollen für AWS WAF](#).

Weitere Informationen zur Erstellung Ihres Lieferdatenstroms finden Sie unter [Erstellen eines Amazon Data Firehose-Lieferdatenstroms](#).

Amazon-Simple-Storage-Service-Buckets

In diesem Thema finden Sie Informationen zum Senden Ihrer Web-ACL-Datenverkehrsprotokolle an einen Amazon-S3-Bucket.

Der Bucket, den Sie als Logging-Ziel wählen, muss einem Firewall Manager Manager-Administratorkonto gehören. Informationen zu den Anforderungen für die Erstellung Ihres Amazon S3

S3-Buckets für die Protokollierung und zu den Anforderungen zur Bucket-Benennung finden Sie unter [Amazon Simple Storage Service](#) im AWS WAF Entwicklerhandbuch.

Letztendliche Datenkonsistenz

Wenn Sie AWS WAF Richtlinien ändern, die mit einem Amazon S3 S3-Protokollierungsziel konfiguriert sind, aktualisiert Firewall Manager die Bucket-Richtlinie, um die für die Protokollierung erforderlichen Berechtigungen hinzuzufügen. Dabei folgt Firewall Manager den last-writer-wins Semantik- und Datenkonsistenzmodellen, denen Amazon Simple Storage Service folgt. Wenn Sie in der Firewall Manager Manager-Konsole oder über die [PutPolicy](#)API mehrere Richtlinienaktualisierungen für ein Amazon S3 S3-Ziel gleichzeitig vornehmen, werden einige Berechtigungen möglicherweise nicht gespeichert. Weitere Informationen zum Amazon S3 S3-Datenkonsistenzmodell finden Sie unter [Amazon S3 S3-Datenkonsistenzmodell](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Berechtigungen zum Veröffentlichen von Protokollen in einem Amazon S3 S3-Bucket

Für die Konfiguration der Web-ACL-Datenverkehrsprotokollierung für einen Amazon S3 S3-Bucket in einer AWS WAF Richtlinie sind die folgenden Berechtigungseinstellungen erforderlich. Firewall Manager fügt diese Berechtigungen automatisch Ihrem Amazon S3-Bucket zu, wenn Sie Amazon S3 als Ihr Protokollierungsziel konfigurieren, um dem Service die Erlaubnis zu erteilen, Protokolle im Bucket zu veröffentlichen. Wenn Sie den Zugriff auf Ihre Protokollierungs- und Firewall Manager Manager-Ressourcen detaillierter verwalten möchten, können Sie diese Berechtigungen selbst festlegen. Informationen zur Verwaltung von Berechtigungen finden Sie unter [Zugriffsverwaltung für AWS Ressourcen](#) im IAM-Benutzerhandbuch. Informationen zu den AWS WAF verwalteten Richtlinien finden Sie unter [AWS verwaltete Richtlinien für AWS WAF](#).

```
{
  "Version": "2012-10-17",
  "Id": "AWSLogDeliveryForFirewallManager",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryAc1CheckFMS",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAc1",
      "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"
      }
    }
  }
]
}

```

Um das Problem der dienstübergreifenden Verwirrung des Deputy zu vermeiden, können Sie der Richtlinie Ihres Buckets die Kontextschlüssel [aws:SourceArn](#) und die [aws:SourceAccount](#) globale Bedingung hinzufügen. Um diese Schlüssel hinzuzufügen, können Sie entweder die Richtlinie ändern, die Firewall Manager für Sie erstellt, wenn Sie das Protokollierungsziel konfigurieren, oder, wenn Sie eine detaillierte Kontrolle wünschen, können Sie Ihre eigene Richtlinie erstellen. Wenn Sie diese Bedingungen zu Ihrer Zielrichtlinie für die Protokollierung hinzufügen, überprüft oder überwacht Firewall Manager die Schutzmaßnahmen für verwirrte Stellvertreter nicht. Allgemeine Informationen zum Problem mit dem verwirrten Stellvertreter finden Sie unter [Das Problem mit dem verwirrten Stellvertreter](#) im IAM-Benutzerhandbuch.

Wenn Sie die hinzugefügten `sourceArn` Eigenschaften `sourceAccount` hinzufügen, wird die Größe der Bucket-Richtlinie erhöht. Wenn Sie eine lange Liste von `sourceArn` Hinzufügeeigenschaften `sourceAccount` hinzufügen, achten Sie darauf, das [Größenkontingent der Amazon S3 S3-Bucket-Richtlinie](#) nicht zu überschreiten.

Das folgende Beispiel zeigt, wie Sie das Problem mit dem verwirrten Stellvertreter verhindern können, indem Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globale Bedingung in der Richtlinie Ihres Buckets verwenden. `member-account-id` Ersetzen Sie es durch die Konto-IDs der Mitglieder in Ihrer Organisation.

```

{
  "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:"
        ]
      }
    }
  }
}

```



```

    }
  }
]
}

```

Serverseitige Verschlüsselung für Amazon S3 S3-Buckets

Sie können die serverseitige Amazon S3 S3-Verschlüsselung aktivieren oder einen vom AWS Key Management Service Kunden verwalteten Schlüssel für Ihren S3-Bucket verwenden. Wenn Sie sich dafür entscheiden, die standardmäßige Amazon S3 S3-Verschlüsselung in Ihrem Amazon S3 S3-Bucket für AWS WAF Protokolle zu verwenden, müssen Sie keine besonderen Maßnahmen ergreifen. Wenn Sie sich jedoch dafür entscheiden, einen vom Kunden bereitgestellten Verschlüsselungsschlüssel zu verwenden, um Ihre Amazon S3 S3-Daten im Ruhezustand zu verschlüsseln, müssen Sie Ihrer AWS Key Management Service Schlüsselrichtlinie die folgende Berechtigungserklärung hinzufügen:

```

{
    "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": "*"
}


```

Informationen zur Verwendung von vom Kunden bereitgestellten Verschlüsselungsschlüsseln mit Amazon S3 finden Sie unter [Verwenden der serverseitigen Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln \(SSE-C\)](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Aktivieren der Protokollierung

Das folgende Verfahren beschreibt, wie die Protokollierung für eine AWS WAF Richtlinie in der Firewall Manager Manager-Konsole aktiviert wird.

Um die Protokollierung für eine AWS WAF Richtlinie zu aktivieren

1. Bevor Sie die Protokollierung aktivieren können, müssen Sie Ihre Zielressourcen für die Protokollierung wie folgt konfigurieren:
 - Amazon Kinesis Data Streams — Erstellen Sie eine Amazon Data Firehose mit Ihrem Firewall Manager Manager-Administratorkonto. Verwenden Sie einen Namen, der mit dem Präfix beginnt. `aws-waf-logs-` z. B. `aws-waf-logs-firewall-manager-central`. Erstellen Sie die Datenquelle mit einer PUT Quelle und in der Region, in der Sie tätig sind. Wenn Sie Logs für Amazon erfassen CloudFront, erstellen Sie die Firehose in USA East (Nord-Virginia). Bevor Sie ihn verwenden, testen Sie Ihren Lieferstream, um sicherzustellen, dass er über einen ausreichenden Durchsatz verfügt, um die Logs Ihrer Organisation zu speichern. Weitere Informationen finden Sie unter [Erstellen eines Amazon Data Firehose-Lieferdatenstroms](#).
 - Amazon Simple Storage Service-Buckets — Erstellen Sie einen Amazon S3 S3-Bucket gemäß den Richtlinien im Thema [Amazon Simple Storage Service](#) im AWS WAF Entwicklerhandbuch. Sie müssen Ihren Amazon S3 S3-Bucket auch mit den unter aufgeführten Berechtigungen konfigurieren [Berechtigungen zum Veröffentlichen von Protokollen in einem Amazon S3 S3-Bucket](#).
 2. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).
-  **Note**

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).
3. Wählen Sie im Navigationsbereich die Option Sicherheitsrichtlinien aus.
 4. Wählen Sie die AWS WAF Richtlinie aus, für die Sie die Protokollierung aktivieren möchten. Weitere Informationen zur AWS WAF -Protokollierung finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).
 5. Wählen Sie auf der Registerkarte Richtliniendetails im Abschnitt Richtlinienregeln die Option Bearbeiten aus.
 6. Wählen Sie für die Konfiguration der Protokollierung die Option Protokollierung aktivieren aus, um die Protokollierung zu aktivieren. Die Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. Wählen Sie das Logging-Ziel und

anschließend das von Ihnen konfigurierte Logging-Ziel aus. Sie müssen ein Protokollierungsziel auswählen, dessen Name mit `aws-waf-logs-` beginnt. Informationen zur Konfiguration eines AWS WAF Protokollierungsziels finden Sie unter [Konfiguration der Protokollierung für eine Richtlinie AWS WAF](#).

7. (Optional) Wenn Sie nicht möchten, dass bestimmte Felder und deren Werte in den Protokollen enthalten sind, machen Sie diese Felder unkenntlich. Wählen Sie das Feld aus, das unkenntlich gemacht werden soll, und klicken Sie dann auf Add (Hinzufügen). Wiederholen Sie diesen Vorgang nach Bedarf, um zusätzliche Felder unkenntlich zu machen. Die unkenntlich gemachten Felder werden als REDACTED in den Protokollen angezeigt. Wenn Sie beispielsweise das Feld URI unkenntlich machen, wird das Feld URI in den Protokollen als REDACTED angezeigt.
8. (Optional) Wenn Sie nicht alle Anforderungen an die Protokolle senden möchten, fügen Sie Filterkriterien und -verhalten hinzu. Wählen Sie unter Filter logs (Protokolle filtern) für jeden Filter, den Sie anwenden möchten, Add filter (Filter hinzufügen) aus. Wählen Sie dann Ihre Filterkriterien und geben Sie an, ob Sie Anforderungen, die den Kriterien entsprechen, beibehalten oder löschen möchten. Wenn Sie mit dem Hinzufügen von Filtern fertig sind, ändern Sie bei Bedarf das Standardprotokollierungsverhalten. Weitere Informationen finden Sie unter [Verwalten der Protokollierung für eine Web-ACL](#) im AWS WAF -Entwicklerhandbuch.
9. Wählen Sie Weiter aus.
10. Überprüfen Sie Ihre Einstellungen und wählen Sie dann Speichern, um Ihre Änderungen an der Richtlinie zu speichern.

Deaktivieren der Protokollierung

Das folgende Verfahren beschreibt, wie Sie die Protokollierung für eine AWS WAF Richtlinie in der Firewall Manager Manager-Konsole deaktivieren.

Um die Protokollierung für eine AWS WAF Richtlinie zu deaktivieren

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich die Option Sicherheitsrichtlinien aus.
3. Wählen Sie die AWS WAF Richtlinie aus, für die Sie die Protokollierung deaktivieren möchten.
4. Wählen Sie auf der Registerkarte Richtliniendetails im Abschnitt Richtlinienregeln die Option Bearbeiten aus.
5. Wählen Sie für den Status der Protokollierung der Konfiguration die Option Deaktiviert aus.
6. Wählen Sie Weiter aus.
7. Überprüfen Sie Ihre Einstellungen und wählen Sie dann Speichern, um Ihre Änderungen an der Richtlinie zu speichern.

AWS Shield Advanced Richtlinien

In einer Firewall Manager AWS Shield Manager-Richtlinie wählen Sie die Ressourcen aus, die Sie schützen möchten. Wenn Sie die Richtlinie mit aktivierter auto Korrektur anwenden, ordnet Firewall Manager für jede Ressource im Geltungsbereich, die noch keiner AWS WAF Web-ACL zugeordnet ist, eine leere AWS WAF Web-ACL zu. Die leere Web-ACL wird für Shield-Überwachungszwecke verwendet. Wenn Sie der Ressource dann eine andere Web-ACL zuordnen, entfernt Firewall Manager die leere Web-ACL-Zuordnung.

Note

Wenn eine Ressource, die in den Geltungsbereich einer AWS WAF Richtlinie fällt, in den Geltungsbereich einer Shield Advanced-Richtlinie fällt, die mit [automatischer DDoS-Abwehr auf Anwendungsebene](#) konfiguriert ist, wendet Firewall Manager den Shield Advanced-Schutz erst an, nachdem die durch die Richtlinie erstellte Web-ACL zugeordnet wurde. AWS WAF

So werden nicht verknüpfte Web-ACLs in Shield-Richtlinien AWS Firewall Manager verwaltet

Sie können über die Einstellung Nicht verknüpfte Web-ACLs verwalten in Ihrer Richtlinie oder über die Einstellung im [SecurityServicePolicyData](#) Datentyp in der API konfigurieren, ob Firewall Manager nicht verknüpfte Web-ACLs für Sie verwaltet. `optimizeUnassociatedWebACLs` Wenn Sie die Verwaltung nicht zugeordneter Web-ACLs in Ihrer Richtlinie aktivieren, erstellt Firewall Manager Web-ACLs in den Konten innerhalb des Richtlinienbereichs nur, wenn die Web-ACLs von mindestens einer Ressource verwendet werden. Wenn ein Konto zu irgendeinem Zeitpunkt in den Geltungsbereich der Richtlinie fällt, erstellt Firewall Manager automatisch eine Web-ACL in dem Konto, sofern mindestens eine Ressource die Web-ACL verwendet.

Wenn Sie die Verwaltung nicht verknüpfter Web-ACLs aktivieren, führt Firewall Manager eine einmalige Bereinigung der nicht verknüpften Web-ACLs in Ihrem Konto durch. Der Bereinigungsprozess kann mehrere Stunden dauern. Wenn eine Ressource den Richtlinienbereich verlässt, nachdem Firewall Manager eine Web-ACL erstellt hat, trennt Firewall Manager die Ressource nicht von der Web-ACL. Wenn Sie möchten, dass Firewall Manager die Web-ACL bereinigt, müssen Sie zuerst die Ressourcen manuell von der Web-ACL trennen und dann die Option Nicht zugeordnete Web-ACLs verwalten in Ihrer Richtlinie aktivieren.

Wenn Sie diese Option nicht aktivieren, verwaltet Firewall Manager keine nicht verknüpften Web-ACLs, und Firewall Manager erstellt automatisch eine Web-ACL für jedes Konto, das innerhalb des Richtlinienbereichs liegt.

Wie geht man AWS Firewall Manager mit Umfangsänderungen der Shield-Richtlinien um?

Konten und Ressourcen können aufgrund einer Reihe von Änderungen, wie z. B. Änderungen an den Einstellungen des Richtlinienbereichs, Änderungen an den Tags auf einer Ressource und der Entfernung eines Kontos aus einer Organisation, den Geltungsbereich einer AWS Firewall Manager Shield Advanced-Richtlinie verlassen. Allgemeine Informationen zu den Einstellungen für den Geltungsbereich von Richtlinien finden Sie unter [AWS Firewall Manager Geltungsbereich der Politik](#).

Bei einer AWS Firewall Manager Shield Advanced-Richtlinie beendet Firewall Manager die Überwachung des Kontos oder der Ressource, wenn ein Konto oder eine Ressource den Gültigkeitsbereich überschreitet.

Wenn ein Konto nicht mehr gültig ist, weil es aus der Organisation entfernt wird, wird es weiterhin Shield Advanced abonniert. Da das Konto nicht mehr Teil der konsolidierten Fakturierungsfamilie

ist, fällt für das Konto eine anteilige Shield Advanced-Abonnementgebühr an. Auf der anderen Seite fallen für ein Konto, das nicht mehr in den Geltungsbereich fällt, aber in der Organisation verbleibt, keine zusätzlichen Gebühren an.

Wenn eine Ressource den Geltungsbereich überschreitet, wird sie weiterhin durch Shield Advanced geschützt und es fallen weiterhin Shield Advanced-Datenübertragungsgebühren an.

Automatische DDoS-Abwehr auf Anwendungsebene

Wenn Sie eine Shield Advanced-Richtlinie auf CloudFront Amazon-Distributionen oder Application Load Balancers anwenden, haben Sie die Möglichkeit, die automatische DDoS-Abwehr von Shield Advanced auf Anwendungsebene in der Richtlinie zu konfigurieren.

Informationen zur automatischen Abwehr von Shield Advanced finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#).

Für die automatische DDoS-Abwehr auf Anwendungsebene von Shield Advanced gelten die folgenden Anforderungen:

- Die automatische DDoS-Abwehr auf Anwendungsebene funktioniert nur mit CloudFront Amazon-Distributionen und Application Load Balancers.

Wenn Sie Ihre Shield Advanced-Richtlinie auf CloudFront Amazon-Distributionen anwenden, können Sie diese Option für Shield Advanced-Richtlinien wählen, die Sie für die globale Region erstellen. Wenn Sie Schutzmaßnahmen auf Application Load Balancers anwenden, können Sie die Richtlinie auf jede Region anwenden, die Firewall Manager unterstützt.

- Die automatische DDoS-Abwehr auf Anwendungsebene funktioniert nur mit Web-ACLs, die mit der neuesten Version von (v2) erstellt wurden. AWS WAF

Aus diesem Grund müssen Sie, wenn Sie über eine Richtlinie verfügen, die AWS WAF klassische Web-ACLs verwendet, entweder die Richtlinie durch eine neue Richtlinie ersetzen, die automatisch die neueste Version von verwendet AWS WAF, oder Firewall Manager eine neue Version von Web-ACLs für Ihre bestehende Richtlinie erstellen lassen und zu deren Verwendung wechseln. Weitere Informationen zu diesen Optionen finden Sie unter [Ersetzen Sie AWS WAF klassische Web-ACLs durch Web-ACLs der neuesten Version](#).

Konfiguration der automatischen Schadensbegrenzung

Die Option zur automatischen DDoS-Abwehr auf Anwendungsebene für Firewall Manager Shield Advanced-Richtlinien wendet die automatische Abwehr von Shield Advanced auf die Konten und

Ressourcen Ihrer Richtlinie an, die in den Geltungsbereich Ihrer Richtlinie fallen. Ausführliche Informationen zu dieser Shield Advanced-Funktion finden Sie unter [Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene](#).

Sie können wählen, ob Firewall Manager die automatische Risikominderung für die CloudFront Distributionen oder Application Load Balancer aktiviert oder deaktiviert, die in den Geltungsbereich der Richtlinie fallen, oder Sie können festlegen, dass die Richtlinie die automatischen Risikominderungseinstellungen von Shield Advanced ignoriert:

- **Aktivieren** — Wenn Sie die automatische Abwehr aktivieren möchten, geben Sie auch an, ob bei der Abwehr von Shield Advanced-Regeln übereinstimmende Webanfragen gezählt oder blockiert werden sollen. Firewall Manager markiert Ressourcen im Geltungsbereich als nicht konform, wenn für sie entweder keine automatische Schadensbegrenzung aktiviert ist oder wenn sie eine Regelaktion verwenden, die nicht der von Ihnen für die Richtlinie angegebenen entspricht. Wenn Sie die Richtlinie für die automatische Behebung konfigurieren, aktualisiert Firewall Manager nicht konforme Ressourcen nach Bedarf.
- **Deaktivieren** — Wenn Sie sich dafür entscheiden, die automatische Risikominderung zu deaktivieren, markiert Firewall Manager Ressourcen im Geltungsbereich als nicht konform, wenn für sie die automatische Risikominderung aktiviert ist. Wenn Sie die Richtlinie für die automatische Behebung konfigurieren, aktualisiert Firewall Manager nicht konforme Ressourcen nach Bedarf.
- **Ignorieren** — Wenn Sie sich dafür entscheiden, die automatische Risikominderung zu ignorieren, berücksichtigt Firewall Manager keine der Einstellungen für die automatische Risikominderung in Ihrer Shield-Richtlinie, wenn er Behebungsaktivitäten für die Richtlinie durchführt. Mit dieser Einstellung können Sie die automatische Abwehr über Shield Advanced steuern, ohne dass diese Einstellungen vom Firewall Manager überschrieben werden. Diese Einstellung gilt nicht für Classic Load Balancer- oder Elastic IP-Ressourcen, die über Shield Advanced verwaltet werden, da Shield Advanced derzeit keine automatische L7-Abwehr für diese Ressourcen unterstützt.

Ersetzen Sie AWS WAF klassische Web-ACLs durch Web-ACLs der neuesten Version

Die automatische DDoS-Abwehr auf Anwendungsebene funktioniert nur mit Web-ACLs, die mit der neuesten Version von AWS WAF (v2) erstellt wurden.

Informationen zur Bestimmung der Web-ACL-Version für Ihre Shield Advanced-Richtlinie finden Sie unter [Ermitteln der Version AWS WAF , die von einer Shield Advanced-Richtlinie verwendet wird](#).

Wenn Sie die automatische Abwehr in Ihrer Shield Advanced-Richtlinie verwenden möchten und Ihre Richtlinie derzeit AWS WAF klassische Web-ACLs verwendet, können Sie entweder eine neue Shield Advanced-Richtlinie erstellen, die Ihre aktuelle ersetzt, oder Sie können die in diesem Abschnitt beschriebenen Optionen verwenden, um Web-ACLs früherer Versionen durch neue (v2) Web-ACLs innerhalb Ihrer aktuellen Shield Advanced-Richtlinie zu ersetzen. Neue Richtlinien erstellen Web-ACLs immer mit der neuesten Version von AWS WAF. Wenn Sie die gesamte Richtlinie ersetzen und sie löschen, können Sie festlegen, dass Firewall Manager auch alle Web-ACLs der früheren Version löscht. Im Rest dieses Abschnitts werden Ihre Optionen zum Ersetzen der Web-ACLs innerhalb Ihrer bestehenden Richtlinie beschrieben.

Wenn Sie eine bestehende Shield Advanced-Richtlinie für CloudFront Amazon-Ressourcen ändern, kann Firewall Manager automatisch eine neue leere AWS WAF (v2) Web-ACL für die Richtlinie erstellen, und zwar für jedes Konto im Geltungsbereich, das noch nicht über eine v2-Web-ACL verfügt. Wenn Firewall Manager eine neue Web-ACL erstellt und die Richtlinie bereits über eine AWS WAF klassische Web-ACL in demselben Konto verfügt, konfiguriert Firewall Manager die Web-ACL der neuen Version mit derselben Standardaktionseinstellung wie die vorhandene Web-ACL. Wenn keine AWS WAF klassische Web-ACL vorhanden ist, legt Firewall Manager die Standardaktion Allow in der neuen Web-ACL auf fest. Nachdem Firewall Manager eine neue Web-ACL erstellt hat, können Sie sie über die AWS WAF Konsole nach Bedarf anpassen.

Wenn Sie eine der folgenden Richtlinienkonfigurationsoptionen wählen, erstellt Firewall Manager neue (v2) Web-ACLs für in den Geltungsbereich fallende Konten, für die sie noch nicht vorhanden sind:

- Wenn Sie die automatische DDoS-Abwehr auf Anwendungsebene aktivieren oder deaktivieren. Diese Wahl allein veranlasst den Firewall Manager lediglich, die neuen Web-ACLs zu erstellen und keine vorhandenen AWS WAF klassischen Web-ACLs auf den Ressourcen zu ersetzen, die in den Geltungsbereich der Richtlinie fallen.
- Wenn Sie sich für die Richtlinienaktion „Automatische Wiederherstellung“ entscheiden und die Option wählen, AWS WAF klassische Web-ACLs durch AWS WAF (v2) -Web-ACLs zu ersetzen. Sie können wählen, ob Sie Web-ACLs früherer Versionen unabhängig von Ihren Konfigurationsoptionen für die automatische DDoS-Abwehr auf Anwendungsebene ersetzen möchten.

Wenn Sie die Ersatzoption wählen, erstellt Firewall Manager die Web-ACLs der neuen Version nach Bedarf und führt dann die folgenden Schritte für die in den Geltungsbereich der Richtlinie fallenden Ressourcen aus:

- Wenn eine Ressource mit einer Web-ACL aus einer anderen aktiven Firewall Manager-Richtlinie verknüpft ist, lässt Firewall Manager die Zuordnung unverändert.
- In allen anderen Fällen entfernt Firewall Manager jegliche Zuordnung zu einer AWS WAF klassischen Web-ACL und ordnet die Ressource der Web-ACL AWS WAF (v2) der Richtlinie zu.

Sie können festlegen, dass Firewall Manager die Web-ACLs der früheren Version durch die Web-ACLs der neuen Version ersetzt, wenn Sie möchten. Wenn Sie die AWS WAF klassischen Web-ACLs der Richtlinie zuvor angepasst haben, können Sie die Web-ACLs der neuen Version auf vergleichbare Einstellungen aktualisieren, bevor Sie festlegen, dass Firewall Manager den Schritt zum Ersetzen durchführt.

Sie können auf beide Versionen von Web-ACL für eine Richtlinie über dieselbe Version der Konsole für oder Classic zugreifen. AWS WAF AWS WAF

Firewall Manager löscht keine ersetzten AWS WAF Classic-Web-ACLs, bis Sie die Richtlinie selbst löschen. Wenn die AWS WAF klassischen Web-ACLs nicht mehr von der Richtlinie verwendet werden, können Sie sie bei Bedarf löschen.

Ermitteln der Version AWS WAF , die von einer Shield Advanced-Richtlinie verwendet wird

Sie können feststellen, welche Version AWS WAF Ihrer Firewall Manager Shield Advanced-Richtlinie verwendet, indem Sie sich die Parameterschlüssel in der AWS Config serviceverknüpften Regel der Richtlinie ansehen. Wenn es sich bei der verwendeten AWS WAF Version um die neueste Version handelt, enthalten die Parameterschlüssel `policyId` und `webACLArn`. Wenn es sich um die frühere Version, AWS WAF Classic, handelt, enthalten die Parameterschlüssel `webACLId` und `resourceTypes`.

AWS Config In der Regel werden nur Schlüssel für die Web-ACLs aufgeführt, die die Richtlinie derzeit mit Ressourcen innerhalb des Gültigkeitsbereichs verwendet.

So ermitteln Sie, welche Version AWS WAF Ihrer Firewall Manager Shield Advanced-Richtlinie verwendet

1. Rufen Sie die Richtlinien-ID für die Shield Advanced-Richtlinie ab:
 - a. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole

unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

- b. Wählen Sie im Navigationsbereich die Option Sicherheitsrichtlinien aus.
- c. Wählen Sie die Region für die Richtlinie aus. Für CloudFront Distributionen ist Global dies.
- d. Suchen Sie die gewünschte Richtlinie und kopieren Sie den Wert der zugehörigen Richtlinien-ID.

Beispiel für eine Richtlinien-ID:1111111-2222-3333-4444-a55aa5aaa555.

2. Erstellen Sie den AWS Config Regelnamen der Richtlinie, indem Sie die Richtlinien-ID an die Zeichenfolge FMManagedShieldConfigRule anhängen.

Beispiel für einen AWS Config

Regelnamen:FMManagedShieldConfigRule1111111-2222-3333-4444-a55aa5aaa555.

3. Suchen Sie in den Parametern für die zugehörige AWS Config Regel nach Schlüsseln mit den Namen `policyId` und `webAclArn`:
 - a. Öffnen Sie die AWS Config Konsole unter <https://console.aws.amazon.com/config/>.
 - b. Wählen Sie im Navigationsbereich Regeln aus.
 - c. Suchen Sie den AWS Config Regelnamen Ihrer Firewall Manager Manager-Richtlinie in der Liste und wählen Sie ihn aus. Die Seite der Regel wird geöffnet.
 - d. Sehen Sie sich unter Regeldetails im Abschnitt Parameter die Schlüssel an. Wenn Sie Schlüssel mit dem Namen `policyId` und `findenwebAclArn`, verwendet die Richtlinie Web-ACLs, die mit der neuesten Version von AWS WAF erstellt wurden. Wenn Sie Schlüssel mit dem Namen `webAclId` und `findenresourceTypes`, verwendet die Richtlinie Web-ACLs, die mit der früheren Version Classic erstellt wurden. AWS WAF

Sicherheitsgruppenrichtlinien

Sie können AWS Firewall Manager Sicherheitsgruppenrichtlinien verwenden, um Amazon Virtual Private Cloud-Sicherheitsgruppen für Ihre Organisation in zu verwalten AWS Organizations. Sie können zentral gesteuerte Sicherheitsgruppenrichtlinien auf Ihre gesamte Organisation oder auf eine ausgewählte Teilmenge Ihrer Konten und Ressourcen anwenden. Sie können auch die Sicherheitsgruppenrichtlinien, die in Ihrer Organisation verwendet werden, mit Prüfungs- und Verwendungssicherheitsgruppenrichtlinien überwachen und verwalten.

Firewall Manager verwaltet Ihre Richtlinien kontinuierlich und wendet sie auf Konten und Ressourcen an, sobald sie in Ihrem Unternehmen hinzugefügt oder aktualisiert werden. Weitere Informationen dazu AWS Organizations finden Sie im [AWS Organizations Benutzerhandbuch](#). Informationen zu Amazon Virtual Private Cloud-Sicherheitsgruppen finden Sie unter [Sicherheitsgruppen für Ihre VPC](#) im [Amazon VPC-Benutzerhandbuch](#).

Sie können die Sicherheitsgruppenrichtlinien von Firewall Manager verwenden, um in Ihrer gesamten AWS Organisation Folgendes zu tun:

- Anwenden gemeinsamer Sicherheitsgruppen auf bestimmte Konten und Ressourcen.
- Prüfen von Sicherheitsgruppenregeln, um nicht konforme Regeln zu finden und zu korrigieren.
- Prüfen der Verwendung von Sicherheitsgruppen, um nicht verwendete und redundante Sicherheitsgruppen zu bereinigen.

Dieser Abschnitt beschreibt, wie die Sicherheitsgruppenrichtlinien von Firewall Manager funktionieren, und bietet Anleitungen zu ihrer Verwendung. Verfahren zum Erstellen von Sicherheitsgruppenrichtlinien finden Sie unter [Eine AWS Firewall Manager Richtlinie erstellen](#).

Gemeinsame Sicherheitsgruppenrichtlinien

Mit einer gemeinsamen Sicherheitsgruppenrichtlinie ermöglicht Firewall Manager eine zentral gesteuerte Zuordnung von Sicherheitsgruppen zu Konten und Ressourcen in Ihrem Unternehmen. Sie geben an, wo und wie die Richtlinie in Ihrer Organisation angewendet werden soll.

Sie können gemeinsame Sicherheitsgruppenrichtlinien auf die folgenden Ressourcentypen anwenden:

- Amazon Elastic Compute Cloud (Amazon EC2) -Instanz
- Elastische Netzwerkschnittstelle
- Application Load Balancer
- Classic Load Balancer

Hinweise zur Erstellung einer gemeinsamen Sicherheitsgruppenrichtlinie mithilfe der Konsole finden Sie unter [Erstellen einer gemeinsamen Sicherheitsgruppenrichtlinie](#).

Freigegebene VPCs

Sie können in den Geltungsbereichseinstellungen für eine allgemeine Sicherheitsgruppenrichtlinie auch freigegebene VPCs aufnehmen. Diese Auswahl beinhaltet auch VPCs, die einem anderen Konto gehören und für ein Konto im Geltungsbereich freigegeben werden. VPCs, die Konten im Geltungsbereich gehören, sind immer enthalten. Informationen zu gemeinsam genutzten VPCs finden Sie unter [Arbeiten mit gemeinsam genutzten VPCs](#) im [Amazon VPC-Benutzerhandbuch](#).

Die folgenden Vorbehalte gelten für das Einbeziehen gemeinsam genutzter VPCs. Diese gelten zusätzlich zu den allgemeinen Vorsichtsmaßnahmen für Sicherheitsgruppenrichtlinien unter [Einschränkungen von Sicherheitsgruppenrichtlinien](#)

- Firewall Manager repliziert die primäre Sicherheitsgruppe in die VPCs für jedes in den Geltungsbereich fallende Konto. Bei einer gemeinsam genutzten VPC repliziert Firewall Manager die primäre Sicherheitsgruppe einmal für jedes Konto im Geltungsbereich, mit dem die VPC gemeinsam genutzt wird. Dies kann in einer einzelnen gemeinsam genutzten VPC zu mehreren Replikaten führen.
- Wenn Sie eine neue gemeinsam genutzte VPC erstellen, wird sie in den Details der Sicherheitsgruppenrichtlinie von Firewall Manager erst angezeigt, nachdem Sie mindestens eine Ressource in der VPC erstellt haben, die in den Geltungsbereich der Richtlinie fällt.
- Wenn Sie gemeinsam genutzte VPCs in einer Richtlinie deaktivieren, für die gemeinsam genutzte VPCs aktiviert waren, löscht Firewall Manager in den gemeinsam genutzten VPCs die Replikatsicherheitsgruppen, die keinen Ressourcen zugeordnet sind. Firewall Manager behält die verbleibenden Replikatsicherheitsgruppen bei, verwaltet sie jedoch nicht mehr. Das Entfernen dieser verbleibenden Sicherheitsgruppen erfordert eine manuelle Verwaltung in jeder freigegebenen VPC-Instance.

Primäre Sicherheitsgruppen

Für jede gemeinsame Sicherheitsgruppenrichtlinie geben AWS Firewall Manager Sie eine oder mehrere primäre Sicherheitsgruppen an:

- Primäre Sicherheitsgruppen müssen vom Firewall Manager Manager-Administratorkonto erstellt werden und können sich in jeder Amazon VPC-Instance des Kontos befinden.
- Sie verwalten Ihre primären Sicherheitsgruppen über Amazon Virtual Private Cloud (Amazon VPC) oder Amazon Elastic Compute Cloud (Amazon EC2). Weitere Informationen finden Sie unter [Arbeiten mit Sicherheitsgruppen](#) im [Amazon VPC-Benutzerhandbuch](#).
- Sie können eine oder mehrere Sicherheitsgruppen als primäre Gruppen für eine Firewall Manager Manager-Sicherheitsgruppenrichtlinie benennen. Standardmäßig ist die Anzahl der zulässigen

Sicherheitsgruppen in einer Richtlinie auf eine Sicherheitsgruppe eingeschränkt. Sie können jedoch eine Anforderung zum Erhöhen des Kontingents absenden. Weitere Informationen finden Sie unter [AWS Firewall Manager Kontingente](#).

Richtlinienregeleinstellungen

Sie können eines oder mehrere der folgenden Verhaltensweisen zur Änderungskontrolle für die Sicherheitsgruppen und Ressourcen Ihrer gemeinsamen Sicherheitsgruppenrichtlinie wählen:

- Identifizieren Sie alle Änderungen, die lokale Benutzer an replizierten Sicherheitsgruppen vorgenommen haben, und berichten Sie darüber.
- Trennen Sie alle anderen Sicherheitsgruppen von den AWS Ressourcen, die in den Geltungsbereich der Richtlinie fallen.
- Verteilen Sie Tags von der primären Gruppe an die replizierten Sicherheitsgruppen.

Important

Firewall Manager verteilt keine Systemtags, die von AWS Diensten hinzugefügt wurden, an die Replikat-Sicherheitsgruppen. System-Tags beginnen mit dem Präfix `aws :`. Darüber hinaus aktualisiert Firewall Manager die Tags vorhandener Sicherheitsgruppen nicht und erstellt auch keine neuen Sicherheitsgruppen, wenn die Richtlinie Tags enthält, die mit der Tag-Richtlinie der Organisation in Konflikt stehen. Informationen zu Tag-Richtlinien finden Sie unter [Tag-Richtlinien](#) im AWS Organizations Benutzerhandbuch.

- Verteilen Sie Sicherheitsgruppenreferenzen von der primären Gruppe auf die replizierten Sicherheitsgruppen.

Auf diese Weise können Sie auf einfache Weise allgemeine Regeln für die Referenzierung von Sicherheitsgruppen für alle im Geltungsbereich befindlichen Ressourcen für Instances einrichten, die der VPC der angegebenen Sicherheitsgruppe zugeordnet sind. Wenn Sie diese Option aktivieren, gibt Firewall Manager die Sicherheitsgruppenverweise nur dann weiter, wenn die Sicherheitsgruppen auf Peer-Sicherheitsgruppen in Amazon Virtual Private Cloud verweisen. Wenn die replizierten Sicherheitsgruppen nicht korrekt auf die Peer-Sicherheitsgruppe verweisen, markiert Firewall Manager diese replizierten Sicherheitsgruppen als nicht konform. Informationen zum Referenzieren von Peer-Sicherheitsgruppen in Amazon VPC finden Sie unter [Aktualisieren Sie Ihre Sicherheitsgruppen, um Peer-Sicherheitsgruppen zu referenzieren](#) im [Amazon VPC Peering Guide](#).

Wenn Sie diese Option nicht aktivieren, gibt Firewall Manager keine Sicherheitsgruppenverweise an die Replikatsicherheitsgruppen weiter. Informationen zum VPC-Peering in Amazon VPC finden Sie im Amazon VPC Peering [Guide](#).

Erstellung und Verwaltung von Richtlinien

Wenn Sie Ihre gemeinsame Sicherheitsgruppenrichtlinie erstellen, repliziert Firewall Manager die primären Sicherheitsgruppen auf jede Amazon VPC-Instance innerhalb des Richtlinienbereichs und ordnet die replizierten Sicherheitsgruppen Konten und Ressourcen zu, die in den Geltungsbereich der Richtlinie fallen. Wenn Sie eine primäre Sicherheitsgruppe ändern, leitet Firewall Manager die Änderung an die Replikate weiter.

Wenn Sie eine gemeinsame Sicherheitsgruppenrichtlinie löschen, können Sie auswählen, ob die von der Richtlinie erstellten Ressourcen bereinigt werden sollen. Für allgemeine Sicherheitsgruppen von Firewall Manager sind diese Ressourcen die Replikat-Sicherheitsgruppen. Wählen Sie die Bereinigungsoption, es sei denn, Sie möchten jedes einzelne Replikat manuell verwalten, nachdem die Richtlinie gelöscht wurde. In den meisten Situationen ist die Auswahl der Bereinigungsoption der einfachste Ansatz.

Verwalten von Replikaten

Die Replikat-Sicherheitsgruppen in den Amazon VPC-Instances werden wie andere Amazon VPC-Sicherheitsgruppen verwaltet. Weitere Informationen finden Sie unter [Sicherheitsgruppen für Ihre VPC](#) im [Amazon VPC-Benutzerhandbuch](#).

Inhaltsprüfungssicherheitsgruppenrichtlinien

Verwenden Sie Sicherheitsgruppenrichtlinien für die AWS Firewall Manager Inhaltsüberwachung, um die Regeln, die in den Sicherheitsgruppen Ihres Unternehmens verwendet werden, zu überwachen und Richtlinienaktionen darauf anzuwenden. Die Sicherheitsgruppenrichtlinien für die Inhaltsüberwachung gelten für alle von Kunden erstellten Sicherheitsgruppen, die in Ihrer AWS Organisation verwendet werden, und zwar entsprechend dem von Ihnen in der Richtlinie definierten Geltungsbereich.

Hinweise zur Erstellung einer Sicherheitsgruppenrichtlinie für Inhaltsaudits mithilfe der Konsole finden Sie unter [Erstellen einer Inhaltsprüfungssicherheitsgruppenrichtlinie](#).

Richtlinienbereich-Ressourcentyp

Sie können Gruppenrichtlinien für die Inhaltsüberwachung auf die folgenden Ressourcentypen anwenden:

- Amazon Elastic Compute Cloud (Amazon EC2) -Instanz
- Elastische Netzwerkschnittstelle
- Amazon VPC-Sicherheitsgruppe

Sicherheitsgruppen werden im Geltungsbereich der Richtlinie berücksichtigt, wenn sie sich explizit im Geltungsbereich befinden oder wenn sie Ressourcen zugeordnet sind, die sich im Geltungsbereich befinden.

Optionen für Richtlinienregeln

Sie können entweder verwaltete oder benutzerdefinierte Richtlinienregeln für jede Inhaltsüberwachungsrichtlinie verwenden, aber nicht beide.

- **Verwaltete Richtlinienregeln** — In einer Richtlinie mit verwalteten Regeln können Sie mithilfe von Anwendungs- und Protokolllisten steuern, welche Regeln Firewall Manager prüft und entweder als konform oder nicht konform kennzeichnet. Sie können Listen verwenden, die von Firewall Manager verwaltet werden. Sie können auch Ihre eigenen Anwendungs- und Protokolllisten erstellen und verwenden. Informationen zu diesen Listentypen und Ihren Verwaltungsoptionen für benutzerdefinierte Listen finden Sie unter [Verwaltete Listen](#).
- **Benutzerdefinierte Richtlinienregeln** — In einer Richtlinie mit benutzerdefinierten Richtlinienregeln geben Sie eine vorhandene Sicherheitsgruppe als Überwachungssicherheitsgruppe für Ihre Richtlinie an. Sie können die Regeln für die Audit-Sicherheitsgruppe als Vorlage verwenden, die die Regeln definiert, die Firewall Manager prüft und entweder als konform oder nicht konform kennzeichnet.

Sicherheitsgruppen überwachen

Sie müssen Audit-Sicherheitsgruppen mit Ihrem Firewall Manager Administratorkonto erstellen, bevor Sie sie in Ihrer Richtlinie verwenden können. Sie können Sicherheitsgruppen über Amazon Virtual Private Cloud (Amazon VPC) oder Amazon Elastic Compute Cloud (Amazon EC2) verwalten. Weitere Informationen finden Sie unter [Arbeiten mit Sicherheitsgruppen](#) im [Amazon VPC-Benutzerhandbuch](#).

Eine Sicherheitsgruppe, die Sie für eine Sicherheitsgruppenrichtlinie zur Inhaltsüberwachung verwenden, wird von Firewall Manager nur als Vergleichsreferenz für die Sicherheitsgruppen

verwendet, die in den Geltungsbereich der Richtlinie fallen. Firewall Manager ordnet es keinen Ressourcen in Ihrer Organisation zu.

Die Art und Weise, wie Sie die Regeln in der Audit-Sicherheitsgruppe definieren, hängt von Ihren Entscheidungen in den Einstellungen der Richtlinienregeln ab:

- **Verwaltete Richtlinienregeln** — Bei Einstellungen für verwaltete Richtlinienregeln verwenden Sie eine Auditsicherheitsgruppe, um andere Einstellungen in der Richtlinie außer Kraft zu setzen und Regeln, die andernfalls zu einem anderen Konformitätsergebnis führen könnten, explizit zuzulassen oder abzulehnen.
 - Wenn Sie festlegen, dass die in der Auditsicherheitsgruppe definierten Regeln immer zugelassen werden, gilt jede Regel, die einer Regel entspricht, die in der Auditsicherheitsgruppe definiert ist, unabhängig von den anderen Richtlinieneinstellungen als richtlinienkonform.
 - Wenn Sie festlegen, dass die in der Auditsicherheitsgruppe definierten Regeln immer abgelehnt werden, gilt jede Regel, die mit einer Regel übereinstimmt, die in der Auditsicherheitsgruppe definiert ist, unabhängig von den anderen Richtlinieneinstellungen als nicht richtlinienkonform.
- **Benutzerdefinierte Richtlinienregeln** — Für benutzerdefinierte Richtlinienregeleneinstellungen bietet die Audit-Sicherheitsgruppe ein Beispiel dafür, was in den im Geltungsbereich enthaltenen Sicherheitsgruppenregeln zulässig oder nicht akzeptabel ist:
 - Wenn Sie sich dafür entscheiden, die Verwendung der Regeln zuzulassen, dürfen alle Sicherheitsgruppen, die in den Geltungsbereich fallen, nur Regeln haben, die innerhalb des zulässigen Bereichs der Überwachungssicherheitsgruppenregeln der Richtlinie liegen. In diesem Fall sind die Sicherheitsgruppenregeln der Richtlinie ein Beispiel dafür, was zulässig ist.
 - Wenn Sie sich dafür entscheiden, die Verwendung der Regeln zu verweigern, dürfen alle Sicherheitsgruppen im Geltungsbereich nur Regeln haben, die nicht innerhalb des zulässigen Bereichs der Überwachungssicherheitsgruppenregeln der Richtlinie liegen. In diesem Fall ist die Sicherheitsgruppe der Richtlinie ein Beispiel dafür, was nicht zulässig ist.

Erstellung und Verwaltung von Richtlinien

Wenn Sie eine Prüfungssicherheitsgruppenrichtlinie erstellen, müssen Sie die automatische Korrektur deaktiviert haben. Die empfohlene Vorgehensweise besteht darin, die Auswirkungen der Richtlinienerstellung zu überprüfen, bevor die automatische Korrektur aktiviert wird. Nachdem Sie die erwarteten Auswirkungen überprüft haben, können Sie die Richtlinie bearbeiten und die automatische Korrektur aktivieren. Wenn die automatische Problembehebung aktiviert ist, aktualisiert oder entfernt Firewall Manager Regeln, die in den Geltungsbereich der Sicherheitsgruppen nicht konform sind.

Sicherheitsgruppen, die von einer Prüfungssicherheitsgruppenrichtlinie betroffen sind

Alle Sicherheitsgruppen in Ihrer Organisation, die vom Kunden erstellt wurden, können im Geltungsbereich einer Prüfungssicherheitsgruppenrichtlinie liegen.

Replikat-Sicherheitsgruppen werden nicht vom Kunden erstellt und können sich daher nicht direkt im Bereich einer Prüfungssicherheitsgruppenrichtlinie befinden. Sie können jedoch aufgrund der automatischen Korrekturaktivitäten der Richtlinie aktualisiert werden. Die primäre Sicherheitsgruppe einer gemeinsamen Sicherheitsgruppenrichtlinie wird vom Kunden erstellt und kann sich im Bereich einer Prüfungssicherheitsgruppenrichtlinie befinden. Wenn eine Audit-Sicherheitsgruppenrichtlinie Änderungen an einer primären Sicherheitsgruppe vornimmt, leitet Firewall Manager diese Änderungen automatisch an die Replikat weiter.

Nutzungsprüfungssicherheitsgruppenrichtlinien

Verwenden Sie Sicherheitsgruppenrichtlinien zur AWS Firewall Manager Nutzungsüberwachung, um Ihr Unternehmen auf ungenutzte und redundante Sicherheitsgruppen zu überwachen und optional eine Säuberung durchzuführen. Wenn Sie die automatische Wiederherstellung für diese Richtlinie aktivieren, geht Firewall Manager wie folgt vor:

1. Konsolidierung redundanter Sicherheitsgruppen, wenn Sie diese Option ausgewählt haben.
2. Entfernen nicht verwendeter Sicherheitsgruppen, wenn Sie diese Option ausgewählt haben.

Sie können Sicherheitsgruppenrichtlinien für die Nutzungsüberwachung auf den folgenden Ressourcentyp anwenden:

- Amazon VPC-Sicherheitsgruppe

Hinweise zur Erstellung einer Sicherheitsgruppenrichtlinie für die Nutzungsüberwachung mithilfe der Konsole finden Sie unter [Erstellen einer Nutzungsprüfungssicherheitsgruppenrichtlinie](#).

Wie Firewall Manager redundante Sicherheitsgruppen erkennt und behebt

Damit Sicherheitsgruppen als redundant betrachtet werden können, müssen für sie genau dieselben Regeln festgelegt sein und sie müssen sich in derselben Amazon VPC-Instance befinden.

Um einen redundanten Sicherheitsgruppensatz zu korrigieren, wählt Firewall Manager eine der Sicherheitsgruppen in der Gruppe aus, die beibehalten werden soll, und ordnet sie dann allen

Ressourcen zu, die den anderen Sicherheitsgruppen in der Gruppe zugeordnet sind. Firewall Manager trennt dann die anderen Sicherheitsgruppen von den Ressourcen, denen sie zugeordnet waren, sodass sie nicht mehr verwendet werden.

Note

Wenn Sie sich auch dafür entschieden haben, nicht verwendete Sicherheitsgruppen zu entfernen, erledigt Firewall Manager dies als Nächstes. Möglicherweise werden dadurch die Sicherheitsgruppen entfernt, die sich in der redundanten Gruppe befinden.

Wie Firewall Manager ungenutzte Sicherheitsgruppen erkennt und behebt

Firewall Manager betrachtet eine Sicherheitsgruppe als unbenutzt, wenn beide der folgenden Bedingungen zutreffen:

- Die Sicherheitsgruppe wird von keiner Amazon EC2 EC2-Instance oder Amazon EC2 EC2-Elastic elastic network interface verwendet.
- Firewall Manager hat innerhalb der im Zeitraum der Richtlinienregel angegebenen Anzahl von Minuten kein Konfigurationselement dafür erhalten.

Der Zeitraum für die Richtlinienregel hat eine Standardeinstellung von null Minuten. Sie können den Zeitraum jedoch auf bis zu 365 Tage (525.600 Minuten) erhöhen, um Zeit zu haben, neue Sicherheitsgruppen Ressourcen zuzuordnen.

Important

Wenn Sie eine andere Anzahl von Minuten als den Standardwert Null angeben, müssen Sie indirekte Beziehungen in aktivieren. AWS Config Andernfalls funktionieren Ihre Sicherheitsgruppenrichtlinien für die Nutzungsüberwachung nicht wie vorgesehen. Informationen zu indirekten Beziehungen finden Sie unter [Indirekte Beziehungen AWS Config im AWS Config](#) Entwicklerhandbuch. AWS Config

Firewall Manager behebt ungenutzte Sicherheitsgruppen, indem er sie nach Möglichkeit gemäß Ihren Regeleinstellungen aus Ihrem Konto löscht. Wenn Firewall Manager eine Sicherheitsgruppe nicht löschen kann, wird sie als nicht richtlinienkonform markiert. Firewall Manager kann keine Sicherheitsgruppe löschen, auf die von einer anderen Sicherheitsgruppe verwiesen wird.

Der Zeitpunkt der Behebung hängt davon ab, ob Sie die Standardeinstellung für den Zeitraum oder eine benutzerdefinierte Einstellung verwenden:

- Der Zeitraum ist auf Null gesetzt, die Standardeinstellung — Mit dieser Einstellung gilt eine Sicherheitsgruppe als unbenutzt, sobald sie nicht von einer Amazon EC2 EC2-Instance oder einer elastic network interface verwendet wird.

Bei dieser Einstellung für einen Zeitraum von Null korrigiert Firewall Manager die Sicherheitsgruppe sofort.

- Zeitraum größer als Null — Mit dieser Einstellung gilt eine Sicherheitsgruppe als unbenutzt, wenn sie nicht von einer Amazon EC2 EC2-Instance oder elastic network interface verwendet wird und Firewall Manager innerhalb der angegebenen Anzahl von Minuten kein Konfigurationselement für sie erhalten hat.

Bei einer Einstellung ungleich Null behebt Firewall Manager die Sicherheitsgruppe, nachdem sie 24 Stunden lang im unbenutzten Zustand geblieben ist.

Standardkontenspezifikation

Wenn Sie über die Konsole eine Sicherheitsgruppenrichtlinie für die Nutzungsüberwachung erstellen, wählt Firewall Manager automatisch die Option Die angegebenen Konten ausschließen und alle anderen einbeziehen. Der Dienst fügt dann das Firewall Manager Manager-Administratorkonto in die Liste ein, die ausgeschlossen werden soll. Dies ist der empfohlene Ansatz, mit dem Sie die Sicherheitsgruppen, die zum Firewall Manager Manager-Administratorkonto gehören, manuell verwalten können.

Bewährte Methoden für Sicherheitsgruppenrichtlinien

In diesem Abschnitt werden Empfehlungen zum Verwalten von Sicherheitsgruppen mit AWS Firewall Manager erläutert:

Schließen Sie das Firewall Manager Manager-Administratorkonto aus

Wenn Sie den Geltungsbereich der Richtlinie festlegen, schließen Sie das Firewall Manager Manager-Administratorkonto aus. Wenn Sie eine Nutzungsprüfungssicherheitsgruppenrichtlinie über die Konsole erstellen, ist dies die Standardoption.

Beginnen Sie mit deaktivierter automatischer Korrektur

Bei Content- oder Nutzungsprüfungssicherheitsgruppenrichtlinien sollten Sie die automatische Korrektur deaktivieren. Überprüfen Sie die Richtliniendetails, um festzustellen, welche Auswirkungen die automatische Korrektur haben würde. Wenn Sie sich sicher sind, dass die Änderungen Ihren Wünschen entsprechen, bearbeiten Sie die Richtlinie, um die automatische Korrektur zu aktivieren.

Vermeiden Sie Konflikte, wenn Sie zum Verwalten von Sicherheitsgruppen auch externe Quellen verwenden

Wenn Sie zur Verwaltung von Sicherheitsgruppen ein anderes Tool oder einen anderen Dienst als Firewall Manager verwenden, achten Sie darauf, Konflikte zwischen Ihren Einstellungen in Firewall Manager und den Einstellungen in Ihrer externen Quelle zu vermeiden. Wenn Sie die automatische Korrektur verwenden und Ihre Einstellungen Konflikte verursachen, kann dies zu einer Kette von widersprüchlichen Korrekturen führen, bei der Ressourcen auf beiden Seiten verbraucht werden.

Angenommen, Sie konfigurieren einen anderen Dienst, um eine Sicherheitsgruppe für eine Reihe von AWS Ressourcen zu verwalten, und Sie konfigurieren eine Firewall Manager Manager-Richtlinie, um eine andere Sicherheitsgruppe für einige oder alle derselben Ressourcen zu verwalten. Wenn Sie eine der beiden Seiten so konfigurieren, dass die Zuordnung einer anderen Sicherheitsgruppe zu den Ressourcen des Bereichs nicht zulässig ist, entfernt diese Seite die Zuordnung der Sicherheitsgruppe, die von der anderen Seite aufrechterhalten wird. Wenn beide Seiten auf diese Weise konfiguriert sind, kann dies zu einem Kreislauf widersprüchlicher Dissoziationen und Assoziationen führen.

Nehmen wir außerdem an, Sie erstellen eine Firewall Manager Manager-Überwachungsrichtlinie, um eine Sicherheitsgruppenkonfiguration durchzusetzen, die mit der Sicherheitsgruppenkonfiguration des anderen Dienstes in Konflikt steht. Durch die Firewall Manager Manager-Überwachungsrichtlinie kann diese Sicherheitsgruppe aktualisiert oder gelöscht werden, wodurch sie für den anderen Dienst nicht mehr richtlinientreu ist. Wenn der andere Dienst so konfiguriert ist, dass er alle gefundenen Probleme überwacht und automatisch behebt, erstellt er die Sicherheitsgruppe neu oder aktualisiert sie, wodurch sie erneut nicht mehr den Firewall-Manager-Überwachungsrichtlinien entspricht. Wenn die Firewall Manager Manager-Überwachungsrichtlinie mit automatischer Behebung konfiguriert ist, aktualisiert oder löscht sie erneut die externe Sicherheitsgruppe usw.

Um solche Konflikte zu vermeiden, sollten Sie Konfigurationen zwischen Firewall Manager und externen Quellen erstellen, die sich gegenseitig ausschließen.

Sie können Tagging verwenden, um externe Sicherheitsgruppen von der automatischen Problembehebung durch Ihre Firewall Manager Manager-Richtlinien auszuschließen. Fügen Sie dazu den Sicherheitsgruppen oder anderen Ressourcen ein oder mehrere Tags hinzu, die von

der externen Quelle verwaltet werden. Wenn Sie dann den Geltungsbereich der Firewall Manager Manager-Richtlinie definieren, schließen Sie in Ihrer Ressourcenspezifikation Ressourcen aus, die das oder die Tags haben, die Sie hinzugefügt haben.

Ebenso sollten Sie in Ihrem externen Tool oder Dienst die von Firewall Manager verwalteten Sicherheitsgruppen von allen Verwaltungs- oder Überwachungsaktivitäten ausschließen. Importieren Sie die Firewall Manager Manager-Ressourcen entweder nicht oder verwenden Sie Firewall Manager-spezifisches Tagging, um sie von der externen Verwaltung auszuschließen.

Bewährte Methoden für die Nutzungsprüfung und Sicherheitsgruppenrichtlinien

Beachten Sie diese Richtlinien, wenn Sie Sicherheitsgruppenrichtlinien für die Nutzungsüberwachung verwenden.

- Vermeiden Sie es, innerhalb kurzer Zeit, z. B. innerhalb eines Zeitfensters von 15 Minuten, mehrere Änderungen am Zuordnungsstatus einer Sicherheitsgruppe vorzunehmen. Dies kann dazu führen, dass Firewall Manager einige oder alle der entsprechenden Ereignisse verpasst. Ordnen Sie beispielsweise eine Sicherheitsgruppe nicht schnell einer elastic network interface zu oder trennen Sie sie.
- Verwenden Sie den AWS Config Konfigurationsrekorder nicht für Sicherheitsgruppenrichtlinien zur Nutzungsüberwachung. Er wird nicht benötigt und für seine Verwendung fallen zusätzliche AWS Config Gebühren an.

Einschränkungen von Sicherheitsgruppenrichtlinien

In diesem Abschnitt werden die Einschränkungen für die Verwendung von AWS Firewall Manager Sicherheitsgruppenrichtlinien aufgeführt:

- Das Aktualisieren von Sicherheitsgruppen für elastische Amazon EC2 EC2-Netzwerkschnittstellen, die mit dem Fargate-Servicetyp erstellt wurden, wird nicht unterstützt. Sie können jedoch Sicherheitsgruppen für elastische Netzwerkschnittstellen von Amazon ECS mit dem Amazon EC2-Servicetyp aktualisieren.
- Firewall Manager unterstützt keine Sicherheitsgruppen für Amazon EC2 Elastic Network Interfaces, die vom Amazon Relational Database Service erstellt wurden.
- Die Aktualisierung von Amazon ECS Elastic Network Interfaces ist nur für Amazon ECS-Services möglich, die den Rolling Update (Amazon ECS) Deployment Controller verwenden. Für andere Amazon ECS-Bereitstellungscontroller wie CODE_DEPLOY oder externe Controller kann Firewall Manager die elastischen Netzwerkschnittstellen derzeit nicht aktualisieren.

- Bei Sicherheitsgruppen für elastische Netzwerkschnittstellen von Amazon EC2 sind Änderungen an einer Sicherheitsgruppe für Firewall Manager nicht sofort sichtbar. Der Firewall Manager erkennt Änderungen normalerweise innerhalb weniger Stunden, die Erkennung kann sich jedoch um bis zu sechs Stunden verzögern.
- Firewall Manager unterstützt die Aktualisierung von Sicherheitsgruppen in elastischen Netzwerkschnittstellen für Network Load Balancer nicht.
- In gängigen Sicherheitsgruppenrichtlinien gilt Folgendes: Wenn eine gemeinsam genutzte VPC später nicht mehr mit einem Konto geteilt wird, löscht Firewall Manager die Replikat-Sicherheitsgruppen im Konto nicht.
- Wenn Sie bei Sicherheitsgruppenrichtlinien zur Nutzungsüberwachung mehrere Richtlinien mit einer benutzerdefinierten Verzögerungseinstellung erstellen, die alle denselben Geltungsbereich haben, ist die erste Richtlinie mit den Konformitätsergebnissen die Richtlinie, die die Ergebnisse meldet.

Anwendungsfälle für Sicherheitsgruppenrichtlinien

Sie können AWS Firewall Manager allgemeine Sicherheitsgruppenrichtlinien verwenden, um die Host-Firewall-Konfiguration für die Kommunikation zwischen Amazon VPC-Instances zu automatisieren. In diesem Abschnitt werden die Amazon VPC-Standardarchitekturen aufgeführt und beschrieben, wie die einzelnen Architekturen mithilfe der allgemeinen Sicherheitsgruppenrichtlinien von Firewall Manager gesichert werden können. Diese Sicherheitsgruppenrichtlinien können Ihnen helfen, ein einheitliches Regelwerk anzuwenden, um Ressourcen in verschiedenen Konten auszuwählen und Konfigurationen pro Konto in Amazon Elastic Compute Cloud und Amazon VPC zu vermeiden.

Mit den allgemeinen Sicherheitsgruppenrichtlinien von Firewall Manager können Sie nur die EC2-Elastic Network-Schnittstellen taggen, die Sie für die Kommunikation mit Instances in einer anderen Amazon VPC benötigen. Die anderen Instances in derselben Amazon VPC sind dann sicherer und isolierter.

Anwendungsfall: Überwachung und Steuerung von Anfragen an Application Load Balancers und Classic Load Balancers

Sie können eine allgemeine Sicherheitsgruppenrichtlinie von Firewall Manager verwenden, um zu definieren, welche Anfragen Ihre Load Balancer im Geltungsbereich bearbeiten sollen. Sie können dies über die Firewall Manager Manager-Konsole konfigurieren. Nur Anfragen, die den Regeln der Sicherheitsgruppe für eingehende Nachrichten entsprechen, können Ihre Load Balancer

erreichen, und die Load Balancer verteilen nur Anfragen, die den Regeln für ausgehende Nachrichten entsprechen.

Anwendungsfall: Über das Internet zugängliche, öffentliche Amazon VPC

Sie können eine allgemeine Sicherheitsgruppenrichtlinie von Firewall Manager verwenden, um eine öffentliche Amazon-VPC zu sichern, um beispielsweise nur den eingehenden Port 443 zuzulassen. Dies entspricht dem ausschließlichen Zulassen eingehenden HTTPS-Datenverkehrs für eine öffentliche VPC. Sie können öffentliche Ressourcen innerhalb der VPC taggen (z. B. als „PublicVPC“) und dann den Geltungsbereich der Firewall Manager Manager-Richtlinie auf nur Ressourcen mit diesem Tag festlegen. Firewall Manager wendet die Richtlinie automatisch auf diese Ressourcen an.

Anwendungsfall: Öffentliche und private Amazon VPC-Instances

Sie können dieselbe gemeinsame Sicherheitsgruppenrichtlinie für öffentliche Ressourcen verwenden, die im vorherigen Anwendungsfall für über das Internet zugängliche, öffentliche Amazon VPC-Instances empfohlen wurde. Sie können eine zweite gemeinsame Sicherheitsgruppenrichtlinie verwenden, um die Kommunikation zwischen öffentlichen und privaten Ressourcen zu beschränken. Kennzeichnen Sie die Ressourcen in den öffentlichen und privaten Amazon VPC-Instances mit etwas wie "PublicPrivate", um die zweite Richtlinie auf sie anzuwenden. Sie können eine dritte Richtlinie verwenden, um die zulässige Kommunikation zwischen den privaten Ressourcen und anderen Unternehmens- oder privaten Amazon VPC-Instances zu definieren. Für diese Richtlinie können Sie ein anderes identifizierendes Tag für die privaten Ressourcen verwenden.

Anwendungsfall: Hub-and-Spoke-Amazon VPC-Instances

Sie können eine gemeinsame Sicherheitsgruppenrichtlinie verwenden, um die Kommunikation zwischen der Amazon VPC-Hub-Instance und Spoke-Amazon VPC-Instances zu definieren. Sie können eine zweite Richtlinie verwenden, um die Kommunikation von jeder Amazon VPC-Instance mit der Amazon VPC-Hub-Instance zu definieren.

Anwendungsfall: Standard-Netzwerkschnittstelle für Amazon EC2 EC2-Instances

Sie können eine gemeinsame Sicherheitsgruppenrichtlinie verwenden, um nur Standardkommunikationen zuzulassen, z. B. interne SSH- und Patch-/OS-Aktualisierungsservices, und um andere unsichere Kommunikationsformen zu verhindern.

Anwendungsfall: Identifizieren Sie Ressourcen mit offenen Berechtigungen

Sie können eine Prüfungssicherheitsgruppenrichtlinie verwenden, um alle Ressourcen in Ihrer Organisation zu identifizieren, die über die Berechtigung zur Kommunikation mit öffentlichen IP-Adressen oder über IP-Adressen verfügen, die Drittanbietern gehören.

AWS Network Firewall Richtlinien

Sie können AWS Firewall Manager Netzwerk-Firewall-Richtlinien verwenden, um AWS Network Firewall Firewalls für Ihre Amazon Virtual Private Cloud Cloud-VPCs in Ihrer gesamten Organisation in zu verwalten. AWS Organizations Sie können zentral gesteuerte Firewalls auf Ihr gesamtes Unternehmen oder auf eine ausgewählte Teilmenge Ihrer Konten und VPCs anwenden.

Die Network Firewall bietet Schutz vor Netzwerkdatenverkehr für die öffentlichen Subnetze in Ihren VPCs. Firewall Manager erstellt und verwaltet Ihre Firewalls auf der Grundlage des in Ihrer Richtlinie definierten Firewall-Management-Typs. Firewall Manager bietet die folgenden Firewall-Managementmodelle:

- **Verteilt** — Für jedes Konto und jede VPC, die innerhalb des Richtlinienbereichs liegen, erstellt Firewall Manager eine Netzwerk-Firewall-Firewall und verteilt Firewall-Endpunkte in VPC-Subnetzen, um den Netzwerkverkehr zu filtern.
- **Zentralisiert** — Firewall Manager erstellt eine einzige Netzwerk-Firewall-Firewall in einer einzigen Amazon-VPC.
- **Vorhandene Firewalls importieren** — Firewall Manager importiert bestehende Firewalls zur Verwaltung in einer einzigen Firewall Manager Manager-Richtlinie. Sie können zusätzliche Regeln auf die importierten Firewalls anwenden, die gemäß Ihrer Richtlinie verwaltet werden, um sicherzustellen, dass Ihre Firewalls Ihren Sicherheitsstandards entsprechen.

Note

Firewall Manager Network Firewall Firewall-Richtlinien sind Firewall Manager Manager-Richtlinien, mit denen Sie den Netzwerk-Firewall-Schutz für Ihre VPCs in Ihrem Unternehmen verwalten.

Der Netzwerk-Firewall-Schutz wird in Ressourcen im Netzwerk-Firewall-Dienst spezifiziert, die als Firewall-Richtlinien bezeichnet werden.

Informationen zur Verwendung der Network Firewall finden Sie im [AWS Network Firewall Entwicklerhandbuch](#).

In den folgenden Abschnitten werden die Anforderungen für die Verwendung von Firewall Manager Manager-Netzwerk-Firewall-Richtlinien behandelt und deren Funktionsweise beschrieben. Das Verfahren zum Erstellen der Richtlinie finden Sie unter [Eine AWS Firewall Manager Richtlinie erstellen für AWS Network Firewall](#).

Sie müssen die gemeinsame Nutzung von Ressourcen aktivieren

Eine Netzwerk-Firewall-Richtlinie teilt Netzwerkfirewall-Regelgruppen für alle Konten in Ihrer Organisation. Damit dies funktioniert, müssen Sie die gemeinsame Nutzung von Ressourcen für aktiviert haben AWS Organizations. Informationen zum Aktivieren der gemeinsamen Nutzung von Ressourcen finden Sie unter [Gemeinsame Nutzung von Ressourcen für Network Firewall- und DNS-Firewall-Richtlinien](#).

Sie müssen Ihre Netzwerk-Firewall-Regelgruppen definiert haben

Wenn Sie eine neue Netzwerk-Firewall-Richtlinie angeben, definieren Sie die Firewall-Richtlinie genauso wie bei der AWS Network Firewall direkten Verwendung. Sie geben die hinzuzufügenden statusfreien Regelgruppen, standardmäßige statusfreie Aktionen und statusbehaftete Regelgruppen an. Ihre Regelgruppen müssen bereits im Firewall Manager Manager-Administratorkonto vorhanden sein, damit Sie sie in die Richtlinie aufnehmen können. Informationen zum Erstellen von Netzwerkfirewall-Regelgruppen finden Sie unter [AWS Network Firewall Regelgruppen](#).


So erstellt Firewall Manager Firewall-Endpunkte

Der Firewall-Management-Typ in Ihrer Richtlinie bestimmt, wie Firewall Manager Firewalls erstellt. Ihre Richtlinie kann verteilte Firewalls oder eine zentralisierte Firewall einrichten oder Sie können vorhandene Firewalls importieren:

- **Verteilt** — Beim verteilten Bereitstellungsmodell erstellt Firewall Manager Endpunkte für jede VPC, die innerhalb des Richtlinienbereichs liegt. Sie können entweder den Endpunktstandort anpassen, indem Sie angeben, in welchen Availability Zones Firewall-Endpoints erstellt werden sollen, oder Firewall Manager kann automatisch Endpunkte in den Availability Zones mit öffentlichen Subnetzen erstellen. Wenn Sie die Availability Zones manuell auswählen, haben Sie die Möglichkeit, die Anzahl der zulässigen CIDRs pro Availability Zone einzuschränken. Wenn Sie beschließen, dass Firewall Manager die Endpoints automatisch erstellt, müssen Sie auch angeben, ob der Dienst einen einzelnen Endpunkt oder mehrere Firewall-Endpunkte innerhalb Ihrer VPCs erstellt.
- Für mehrere Firewall-Endpunkte stellt Firewall Manager einen Firewall-Endpunkt in jeder Availability Zone bereit, in der Sie ein Subnetz mit einem Internet-Gateway oder einer von

Firewall Manager erstellten Firewall-Endpunktroute in der Routentabelle haben. Dies ist die Standardoption für eine Netzwerk-Firewall-Richtlinie.

- Für einen einzelnen Firewall-Endpunkt stellt Firewall Manager einen Firewall-Endpunkt in einer einzelnen Availability Zone in jedem Subnetz bereit, das über eine Internet-Gateway-Route verfügt. Bei dieser Option muss der Verkehr in anderen Zonen Zonengrenzen überschreiten, um von der Firewall gefiltert zu werden.

 Note

Für beide Optionen muss ein Subnetz mit einer Routing-Tabelle verknüpft sein, die eine IPv4/PrefixList-Route enthält. Firewall Manager sucht nicht nach anderen Ressourcen.

- Zentralisiert — Beim zentralisierten Bereitstellungsmodell erstellt Firewall Manager einen oder mehrere Firewall-Endpunkte innerhalb einer Inspektions-VPC. Eine Inspektions-VPC ist eine zentrale VPC, auf der Firewall Manager Ihre Endgeräte startet. Wenn Sie das zentralisierte Bereitstellungsmodell verwenden, geben Sie auch an, in welchen Availability Zones Firewall-Endpoints erstellt werden sollen. Sie können die Inspektions-VPC nicht ändern, nachdem Sie Ihre Richtlinie erstellt haben. Um eine andere Inspektions-VPC zu verwenden, müssen Sie eine neue Richtlinie erstellen.
- Vorhandene Firewalls importieren — Wenn Sie vorhandene Firewalls importieren, wählen Sie die Firewalls aus, die in Ihrer Richtlinie verwaltet werden sollen, indem Sie Ihrer Richtlinie eine oder mehrere Ressourcensätze hinzufügen. Ein Ressourcensatz ist eine Sammlung von Ressourcen, in diesem Fall bestehende Firewalls in der Network Firewall, die von einem Konto in Ihrer Organisation verwaltet werden. Bevor Sie Ressourcensätze in Ihrer Richtlinie verwenden, müssen Sie zunächst eine Ressourcengruppe erstellen. Informationen zu Firewall Manager Manager-Ressourcensätzen finden Sie unter [Arbeiten mit Ressourcensätzen in Firewall Manager](#).

Beachten Sie bei der Arbeit mit importierten Firewalls die folgenden Überlegungen:

- Wenn eine importierte Firewall nicht mehr konform ist, versucht Firewall Manager, den Verstoß automatisch zu beheben, außer unter den folgenden Umständen:
 - Wenn es eine Diskrepanz zwischen den statusbehafteten oder statusfreien Standardaktionen des Firewall-Managers und der Netzwerk-Firewall-Richtlinie gibt.
 - Wenn eine Regelgruppe in der Firewall-Richtlinie einer importierten Firewall dieselbe Priorität hat wie eine Regelgruppe in der Firewall Manager Manager-Richtlinie.
 - Wenn eine importierte Firewall eine Firewall-Richtlinie verwendet, die mit einer Firewall verknüpft ist, die nicht Teil des Ressourcensatzes der Richtlinie ist. Dies kann passieren,

weil eine Firewall genau eine Firewall-Richtlinie haben kann, eine einzelne Firewall-Richtlinie jedoch mehreren Firewalls zugeordnet werden kann.

- Wenn einer bereits vorhandenen Regelgruppe, die zur Firewall-Richtlinie einer importierten Firewall gehört, die auch in der Firewall Manager Manager-Richtlinie angegeben ist, eine andere Priorität zugewiesen wird.
- Wenn Sie die Ressourcenbereinigung in der Richtlinie aktivieren, entfernt Firewall Manager die Regelgruppen, die in der FMS-Importrichtlinie enthalten waren, aus den Firewalls im Bereich des Ressourcensatzes.
- Firewalls, die von einem Firewall Manager Manager-Import verwaltet werden, der vorhandene Firewall-Managementtyp kann jeweils nur mit einer Richtlinie verwaltet werden. Wenn derselbe Ressourcensatz zu mehreren importierten Netzwerk-Firewall-Richtlinien hinzugefügt wird, werden die Firewalls in der Ressourcengruppe von der ersten Richtlinie verwaltet, zu der der Ressourcensatz hinzugefügt wurde, und von der zweiten Richtlinie ignoriert.
- Firewall Manager streamt derzeit keine Konfigurationen von Ausnahmerichtlinien. Informationen zu Stream-Ausnahmerichtlinien finden Sie unter [Stream-Ausnahmerichtlinie](#) im AWS Network Firewall Entwicklerhandbuch.

Wenn Sie die Liste der Availability Zones für Richtlinien ändern, die verteiltes oder zentrales Firewall-Management verwenden, versucht Firewall Manager, alle Endpoints zu bereinigen, die in der Vergangenheit erstellt wurden, aber derzeit nicht im Geltungsbereich der Richtlinien liegen. Firewall Manager entfernt den Endpunkt nur, wenn es keine Routing-Tabellenrouten gibt, die auf den außerhalb des Gültigkeitsbereichs liegenden Endpunkt verweisen. Wenn Firewall Manager feststellt, dass er diese Endpunkte nicht löschen kann, markiert er das Firewall-Subnetz als nicht konform und versucht weiterhin, den Endpunkt zu entfernen, bis er sicher gelöscht werden kann.

So verwaltet Firewall Manager Ihre Firewall-Subnetze

Firewall-Subnetze sind die VPC-Subnetze, die Firewall Manager für die Firewall-Endpunkte erstellt, die Ihren Netzwerkverkehr filtern. Jeder Firewall-Endpunkt muss in einem dedizierten VPC-Subnetz bereitgestellt werden. Firewall Manager erstellt mindestens ein Firewall-Subnetz in jeder VPC, die in den Geltungsbereich der Richtlinie fällt.

Für Richtlinien, die das verteilte Bereitstellungsmodell mit automatischer Endpunktkonfiguration verwenden, erstellt Firewall Manager nur Firewall-Subnetze in Availability Zones, die ein Subnetz mit einer Internet-Gateway-Route oder ein Subnetz mit einer Route zu den Firewall-Endpunkten haben, die Firewall Manager für ihre Richtlinie erstellt hat. Weitere Informationen finden Sie unter [VPCs und Subnetze](#) im [Amazon VPC-Benutzerhandbuch](#).

Für Richtlinien, die entweder das verteilte oder das zentralisierte Modell verwenden, bei dem Sie angeben, in welchen Availability Zones Firewall Manager die Firewall-Endpoints erstellt, erstellt Firewall Manager einen Endpunkt in diesen spezifischen Availability Zones, unabhängig davon, ob sich andere Ressourcen in der Availability Zone befinden.

Wenn Sie zum ersten Mal eine Netzwerk-Firewall-Richtlinie definieren, geben Sie an, wie Firewall Manager die Firewall-Subnetze in jeder der VPCs verwaltet, die in den Geltungsbereich fallen. Sie können diese Auswahl später nicht mehr ändern.

Für Richtlinien, die das verteilte Bereitstellungsmodell mit automatischer Endpunktkonfiguration verwenden, können Sie zwischen den folgenden Optionen wählen:

- Stellen Sie ein Firewall-Subnetz für jede Availability Zone bereit, die über öffentliche Subnetze verfügt. Dies ist das Standardverhalten. Dadurch wird eine hohe Verfügbarkeit Ihrer Schutzmaßnahmen zur Filterung des Datenverkehrs gewährleistet.
- Stellen Sie ein einzelnes Firewall-Subnetz in einer Availability Zone bereit. Mit dieser Auswahl identifiziert Firewall Manager eine Zone in der VPC mit den meisten öffentlichen Subnetzen und erstellt dort das Firewall-Subnetz. Der einzelne Firewall-Endpunkt filtert den gesamten Netzwerkverkehr für die VPC. Dies kann die Firewallkosten senken, ist aber nicht hochverfügbar und erfordert, dass der Datenverkehr aus anderen Zonen die Zonengrenzen überschreitet, um gefiltert zu werden.

Für Richtlinien, die ein verteiltes Bereitstellungsmodell mit benutzerdefinierter Endpunktkonfiguration oder das zentralisierte Bereitstellungsmodell verwenden, erstellt Firewall Manager die Subnetze in den angegebenen Availability Zones, die innerhalb des Richtlinienbereichs liegen.

Sie können VPC-CIDR-Blöcke bereitstellen, die Firewall Manager für die Firewall-Subnetze verwenden kann, oder Sie können die Auswahl der Firewall-Endpointadressen dem Firewall Manager überlassen.

- Wenn Sie keine CIDR-Blöcke bereitstellen, fragt Firewall Manager Ihre VPCs nach verfügbaren IP-Adressen ab, die verwendet werden können.
- Wenn Sie eine Liste von CIDR-Blöcken bereitstellen, sucht Firewall Manager nur in den CIDR-Blöcken, die Sie angeben, nach neuen Subnetzen. Sie müssen /28 CIDR-Blöcke verwenden. Für jedes Firewall-Subnetz, das Firewall Manager erstellt, durchsucht er Ihre CIDR-Sperlliste und verwendet das erste Subnetz, das für die Availability Zone und VPC gilt und über verfügbare Adressen verfügt. Wenn Firewall Manager keinen freien Speicherplatz in der VPC finden kann (mit oder ohne Einschränkung), erstellt der Dienst keine Firewall in der VPC.

Wenn Firewall Manager ein erforderliches Firewall-Subnetz in einer Availability Zone nicht erstellen kann, markiert er das Subnetz als nicht richtlinienkonform. Solange sich die Zone in diesem Zustand befindet, muss der Datenverkehr für die Zone die Zonengrenzen überschreiten, damit er von einem Endpunkt in einer anderen Zone gefiltert werden kann. Dies ähnelt dem Szenario mit einem einzelnen Firewall-Subnetz.

So verwaltet Firewall Manager Ihre Netzwerk-Firewall-Ressourcen

Wenn Sie die Richtlinie in Firewall Manager definieren, geben Sie das Filterverhalten für den Netzwerkverkehr einer AWS Network Firewall Standard-Firewall-Richtlinie an. Sie fügen statusfreie und statusbehaftete Netzwerk-Firewall-Regelgruppen hinzu und geben Standardaktionen für Pakete an, die keinen statusfreien Regeln entsprechen. [Informationen zur Arbeit mit Firewall-Richtlinien finden Sie in den AWS Network Firewall Firewall-Richtlinien.](#)[AWS Network Firewall](#)

Bei verteilten und zentralisierten Richtlinien erstellt Firewall Manager beim Speichern der Netzwerk-Firewall-Richtlinie eine Firewall und eine Firewall-Richtlinie in jeder VPC, die in den Geltungsbereich der Richtlinie fällt. Firewall Manager benennt diese Netzwerk-Firewall-Ressourcen, indem er die folgenden Werte verkettet:

- Eine feste Zeichenfolge, entweder `FMMangedNetworkFirewall` oder `FMMangedNetworkFirewallPolicy`, abhängig vom Ressourcentyp.
- Name der Firewall Manager Manager-Richtlinie. Dies ist der Name, den Sie bei der Erstellung der Richtlinie vergeben.
- Firewall Manager Manager-Richtlinien-ID. Dies ist die AWS Ressourcen-ID für die Firewall Manager Manager-Richtlinie.
- Amazon VPC-ID. Dies ist die AWS Ressourcen-ID für die VPC, auf der Firewall Manager die Firewall und die Firewall-Richtlinie erstellt.

Im Folgenden sehen Sie einen Beispielnamen für eine Firewall, die von Firewall Manager verwaltet wird:


```
FMMangedNetworkFirewallEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

Im Folgenden wird ein Beispiel für den Namen einer Firewall-Richtlinie gezeigt:

```
FMMangedNetworkFirewallPolicyEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

Nachdem Sie die Richtlinie erstellt haben, können Mitgliedskonten in den VPCs Ihre Firewall-Richtlinieneinstellungen oder Ihre Regelgruppen nicht überschreiben, aber sie können Regelgruppen zu der Firewall-Richtlinie hinzufügen, die Firewall Manager erstellt hat.

So verwaltet und überwacht Firewall Manager VPC-Routing-Tabellen für Ihre Richtlinie

 Note

Die Verwaltung von Routing-Tabellen wird derzeit nicht für Richtlinien unterstützt, die das zentralisierte Bereitstellungsmodell verwenden.

Wenn Firewall Manager Ihre Firewall-Endpoints erstellt, erstellt er auch die VPC-Routing-Tabellen für sie. Firewall Manager verwaltet Ihre VPC-Routing-Tabellen jedoch nicht. Sie müssen Ihre VPC-Routing-Tabellen so konfigurieren, dass der Netzwerkverkehr zu den Firewall-Endpunkten geleitet wird, die von Firewall Manager erstellt wurden. Ändern Sie mithilfe der Verbesserungen des Amazon VPC-Ingress-Routings Ihre Routing-Tabellen, um den Datenverkehr durch die neuen Firewall-Endpunkte zu leiten. Ihre Änderungen müssen die Firewall-Endpunkte zwischen den Subnetzen, die Sie schützen möchten, und externen Standorten einfügen. Das genaue Routing, das Sie durchführen müssen, hängt von Ihrer Architektur und ihren Komponenten ab.

Derzeit ermöglicht Firewall Manager die Überwachung Ihrer VPC-Routingtabellenrouten für jeglichen Datenverkehr, der an das Internet-Gateway gerichtet ist und die Firewall umgeht. Firewall Manager unterstützt keine anderen Ziel-Gateways wie NAT-Gateways.

Informationen zur Verwaltung von Routentabellen für Ihre VPC finden Sie unter [Verwaltung von Routentabellen für Ihre VPC](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Informationen zur Verwaltung Ihrer Routing-Tabellen für die Network Firewall finden Sie unter [Routentabellenkonfigurationen für AWS Network Firewall](#) im AWS Network Firewall Entwicklerhandbuch.

Wenn Sie die Überwachung für eine Richtlinie aktivieren, überwacht Firewall Manager kontinuierlich die VPC-Routenkonfigurationen und warnt Sie vor Datenverkehr, der die Firewall-Inspektion für diese VPC umgeht. Wenn ein Subnetz über eine Firewall-Endpunktroute verfügt, sucht Firewall Manager nach den folgenden Routen:

- Routen zum Senden von Datenverkehr an den Netzwerk-Firewall-Endpunkt.
- Routen zur Weiterleitung des Datenverkehrs vom Netzwerkfirewall-Endpunkt zum Internet-Gateway.

- Eingehende Routen vom Internet-Gateway zum Netzwerk-Firewall-Endpunkt.
- Routen vom Firewall-Subnetz.

Wenn ein Subnetz über eine Netzwerkfirewall-Route verfügt, die Network Firewall und Ihre Internet-Gateway-Routentabelle jedoch asymmetrisches Routing enthält, meldet Firewall Manager das Subnetz als nicht konform. Firewall Manager erkennt auch Routen zum Internet-Gateway in der Firewall-Routentabelle, die Firewall Manager erstellt hat, sowie in der Routing-Tabelle für Ihr Subnetz und meldet sie als nicht konform. Zusätzliche Routen in der Subnetz-Routentabelle der Network Firewall und Ihrer Internet-Gateway-Routentabelle werden ebenfalls als nicht konform gemeldet. Je nach Art des Verstoßes schlägt Firewall Manager Korrekturmaßnahmen vor, um die Routenkonfiguration auf Konformität zu bringen. Firewall Manager bietet nicht in allen Fällen Vorschläge. Wenn Ihr Kundensubnetz beispielsweise über einen Firewall-Endpunkt verfügt, der außerhalb von Firewall Manager erstellt wurde, schlägt Firewall Manager keine Behebungsmaßnahmen vor.

Standardmäßig markiert Firewall Manager jeden Datenverkehr, der die Grenze der Availability Zone zur Überprüfung überschreitet, als nicht konform. Wenn Sie sich jedoch dafür entscheiden, automatisch einen einzelnen Endpunkt in Ihrer VPC zu erstellen, markiert Firewall Manager den Datenverkehr, der die Grenze der Availability Zone überschreitet, nicht als nicht konform.

Bei Richtlinien, die verteilte Bereitstellungsmodelle mit benutzerdefinierter Endpunktkonfiguration verwenden, können Sie wählen, ob der Datenverkehr, der die Availability Zone-Grenze von einer Availability Zone ohne Firewall-Endpunkt überschreitet, als konform oder nicht konform markiert wird.

Note

- Firewall Manager schlägt keine Behebungsmaßnahmen für Nicht-IPv4-Routen vor, z. B. IPv6- und Präfixlistenrouten.
- Die Erkennung von Aufrufen, die über den `DisassociateRouteTable` API-Aufruf getätigt wurden, kann bis zu 12 Stunden dauern.
- Firewall Manager erstellt eine Netzwerk-Firewall-Routentabelle für ein Subnetz, das die Firewall-Endpunkte enthält. Firewall Manager geht davon aus, dass diese Routentabelle nur gültige Internet-Gateway- und VPC-Standardrouten enthält. Alle zusätzlichen oder ungültigen Routen in dieser Routentabelle gelten als nicht konform.

Wenn Sie bei der Konfiguration Ihrer Firewall Manager-Richtlinie den Überwachungsmodus wählen, stellt Firewall Manager Informationen zu Ressourcenverletzungen und Problembehebungen zu Ihren Ressourcen bereit. Sie können diese vorgeschlagenen Behebungsmaßnahmen verwenden, um Routenprobleme in Ihren Routing-Tabellen zu beheben. Wenn Sie den Modus Aus wählen, überwacht Firewall Manager den Inhalt Ihrer Routing-Tabelle nicht für Sie. Mit dieser Option verwalten Sie Ihre VPC-Routing-Tabellen selbst. Weitere Informationen zu diesen Ressourcenverletzungen finden Sie unter [Compliance-Informationen für eine AWS Firewall Manager Richtlinie anzeigen](#).

Warning

Wenn Sie bei der Erstellung Ihrer Richtlinie unter AWS Network Firewall Routenkonfiguration die Option Überwachen auswählen, können Sie die Option für diese Richtlinie nicht deaktivieren. Wenn Sie jedoch Aus wählen, können Sie es später aktivieren.

Die Protokollierung für eine AWS Network Firewall Richtlinie konfigurieren

Sie können die zentrale Protokollierung für Ihre Netzwerk-Firewall-Richtlinien aktivieren, um detaillierte Informationen über den Verkehr innerhalb Ihres Unternehmens zu erhalten. Sie können die Datenflussprotokollierung auswählen, um den Netzwerkdatenfluss zu erfassen, oder die Warnungsprotokollierung, um Datenverkehr zu melden, der einer Regel entspricht, für die die Regelaktion auf DROP oder gesetzt ist ALERT. Weitere Informationen zur AWS Network Firewall Protokollierung finden Sie unter [Protokollieren des Netzwerkverkehrs von AWS Network Firewall](#) im AWS Network Firewall Entwicklerhandbuch.

Sie senden Protokolle von den Netzwerk-Firewall-Firewalls Ihrer Richtlinie an einen Amazon S3 S3-Bucket. Nachdem Sie die Protokollierung aktiviert haben, AWS Network Firewall werden Protokolle für jede konfigurierte Network Firewall bereitgestellt, indem die Firewall-Einstellungen aktualisiert werden, sodass Protokolle an Ihre ausgewählten Amazon S3 S3-Buckets mit dem reservierten AWS Firewall Manager Präfix, <policy-name>-<policy-id> gesendet werden.

Note

Dieses Präfix wird von Firewall Manager verwendet, um festzustellen, ob eine Protokollierungskonfiguration von Firewall Manager oder vom Kontoinhaber hinzugefügt wurde. Wenn der Kontoinhaber versucht, das reservierte Präfix für

seine eigene benutzerdefinierte Protokollierung zu verwenden, wird es durch die Protokollierungskonfiguration in der Firewall Manager Manager-Richtlinie überschrieben.

Weitere Informationen zum Erstellen eines Amazon S3-Buckets und zum Überprüfen der gespeicherten Protokolle finden Sie unter [Was ist Amazon S3?](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Um die Protokollierung zu aktivieren, müssen Sie die folgenden Anforderungen erfüllen:

- Das Amazon S3, das Sie in Ihrer Firewall Manager Manager-Richtlinie angeben, muss vorhanden sein.
- Sie benötigen die folgenden Berechtigungen:
 - `logs:CreateLogDelivery`
 - `s3:GetBucketPolicy`
 - `s3:PutBucketPolicy`
- Wenn der Amazon S3 S3-Bucket, der Ihr Logging-Ziel ist, serverseitige Verschlüsselung mit Schlüsseln verwendet AWS Key Management Service, die in gespeichert sind, müssen Sie Ihrem AWS KMS vom Kunden verwalteten Schlüssel die folgende Richtlinie hinzufügen, damit Firewall Manager sich in Ihrer CloudWatch Logs-Protokollgruppe anmelden kann:

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "delivery.logs.amazonaws.com"
  },
  "Action": [
    "kms:Encrypt*",
    "kms:Decrypt*",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:Describe*"
  ],
  "Resource": "*"
}
```


Beachten Sie, dass nur Buckets im Firewall Manager Manager-Administratorkonto für die AWS Network Firewall zentrale Protokollierung verwendet werden dürfen.

Wenn Sie die zentrale Protokollierung für eine Netzwerk-Firewall-Richtlinie aktivieren, führt Firewall Manager die folgenden Aktionen für Ihr Konto durch:

- Firewall Manager aktualisiert die Berechtigungen für ausgewählte S3-Buckets, um die Protokollzustellung zu ermöglichen.
- Firewall Manager erstellt Verzeichnisse im S3-Bucket für jedes Mitgliedskonto im Geltungsbereich der Richtlinie. Die Protokolle für jedes Konto finden Sie unter `<bucket-name>/<policy-name>-<policy-id>/AWSLogs/<account-id>`.

So aktivieren Sie die Protokollierung für eine Netzwerk-Firewall-Richtlinie

1. Erstellen Sie mit Ihrem Firewall Manager Manager-Administratorkonto einen Amazon S3 S3-Bucket. Weitere Informationen finden Sie unter [Bucket erstellen](#) im Amazon Simple Storage Service-Benutzerhandbuch.
2. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

 Note


Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

3. Wählen Sie im Navigationsbereich die Option Sicherheitsrichtlinien aus.
4. Wählen Sie die Netzwerk-Firewall-Richtlinie aus, für die Sie die Protokollierung aktivieren möchten. Weitere Informationen zur AWS Network Firewall Protokollierung finden Sie AWS Network Firewall im AWS Network Firewall Entwicklerhandbuch unter [Protokollieren von Netzwerkverkehr von](#).
5. Wählen Sie auf der Registerkarte Richtliniendetails im Abschnitt Richtlinienregeln die Option Bearbeiten aus.
6. Um Protokolle zu aktivieren und zu aggregieren, wählen Sie unter Protokollierungskonfiguration eine oder mehrere Optionen aus:

- Aktivieren und aggregieren Sie Flow-Logs
 - Alert-Logs aktivieren und aggregieren
7. Wählen Sie den Amazon S3 S3-Bucket aus, in den Ihre Logs geliefert werden sollen. Sie müssen für jeden Protokolltyp, den Sie aktivieren, einen Bucket auswählen. Sie können denselben Bucket für beide Protokolltypen verwenden.
 8. (Optional) Wenn Sie möchten, dass die benutzerdefinierte, von Mitgliedskonten erstellte Protokollierung durch die Protokollierungskonfiguration der Richtlinie ersetzt wird, wählen Sie „Bestehende Protokollierungskonfiguration überschreiben“.
 9. Wählen Sie Weiter aus.
 10. Überprüfen Sie Ihre Einstellungen und wählen Sie dann Speichern, um Ihre Änderungen an der Richtlinie zu speichern.

So deaktivieren Sie die Protokollierung für eine Netzwerk-Firewall-Richtlinie

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

 Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich die Option Sicherheitsrichtlinien aus.
3. Wählen Sie die Netzwerk-Firewall-Richtlinie aus, für die Sie die Protokollierung deaktivieren möchten.
4. Wählen Sie auf der Registerkarte Richtliniendetails im Abschnitt Richtlinienregeln die Option Bearbeiten aus.
5. Deaktivieren Sie unter Status der Protokollierungskonfiguration die Optionen Flow-Logs aktivieren und aggregieren und Alert-Logs aktivieren und aggregieren, falls sie ausgewählt sind.
6. Wählen Sie Weiter aus.
7. Überprüfen Sie Ihre Einstellungen und wählen Sie dann Speichern, um Ihre Änderungen an der Richtlinie zu speichern.

DNS-Firewall-Richtlinien für Amazon Route 53 Resolver

Sie können AWS Firewall Manager DNS-Firewall-Richtlinien verwenden, um Verknüpfungen zwischen Amazon Route 53 Resolver DNS-Firewall-Regelgruppen und Ihren Amazon Virtual Private Cloud Cloud-VPCs in Ihrer gesamten Organisation zu verwalten. AWS Organizations Sie können zentral gesteuerte Regelgruppen auf Ihre gesamte Organisation oder auf eine ausgewählte Teilmenge Ihrer Konten und VPCs anwenden.

Die DNS-Firewall ermöglicht die Filterung und Regulierung des ausgehenden DNS-Datenverkehrs für Ihre VPCs. Sie erstellen wiederverwendbare Sammlungen von Filterregeln in DNS-Firewall-Regelgruppen und ordnen die Regelgruppen Ihren VPCs zu. Wenn Sie die Firewall Manager-Richtlinie anwenden, erstellt Firewall Manager für jedes Konto und jede VPC, die innerhalb des Richtlinienbereichs liegen, eine Zuordnung zwischen jeder DNS-Firewall-Regelgruppe in der Richtlinie und jeder VPC, die in den Geltungsbereich der Richtlinie fällt. Dabei werden die Einstellungen für die Zuordnungspriorität verwendet, die Sie in der Firewall Manager Manager-Richtlinie angeben.

Informationen zur Verwendung der DNS-Firewall finden Sie unter [Amazon Route 53 Resolver DNS Firewall](#) im [Amazon Route 53 Developer Guide](#).

In den folgenden Abschnitten werden die Anforderungen für die Verwendung der DNS-Firewall-Richtlinien von Firewall Manager behandelt und die Funktionsweise der Richtlinien beschrieben. Das Verfahren zum Erstellen der Richtlinie finden Sie unter [Erstellen einer AWS Firewall Manager Richtlinie für Amazon Route 53 Resolver DNS Firewall](#).

Sie müssen die gemeinsame Nutzung von Ressourcen aktivieren

Eine DNS-Firewall-Richtlinie teilt DNS-Firewall-Regelgruppen für alle Konten in Ihrer Organisation. Damit dies funktioniert, müssen Sie Resource Sharing mit aktiviert haben AWS Organizations. Informationen zum Aktivieren der gemeinsamen Nutzung von Ressourcen finden Sie unter [Gemeinsame Nutzung von Ressourcen für Network Firewall- und DNS-Firewall-Richtlinien](#).

Sie müssen Ihre DNS-Firewall-Regelgruppen definiert haben

Wenn Sie eine neue DNS-Firewall-Richtlinie angeben, definieren Sie die Regelgruppen genauso wie bei der direkten Verwendung der Amazon Route 53 Resolver DNS Firewall. Ihre Regelgruppen müssen bereits im Firewall Manager Manager-Administratorkonto vorhanden sein, damit Sie sie in die Richtlinie aufnehmen können. Informationen zum Erstellen von DNS-Firewall-Regelgruppen finden Sie unter [DNS-Firewall-Regelgruppen und Regeln](#).

Sie definieren die Zuordnungen der Regelgruppen mit der niedrigsten und der höchsten Priorität

Die Zuordnungen von DNS-Firewall-Regelgruppen, die Sie über die DNS-Firewall-Richtlinien von Firewall Manager verwalten, enthalten die Zuordnungen mit der niedrigsten Priorität und die Zuordnungen mit der höchsten Priorität für Ihre VPCs. In Ihrer Richtlinienkonfiguration werden diese als erste und letzte Regelgruppe angezeigt.

Die DNS-Firewall filtert den DNS-Verkehr für die VPC in der folgenden Reihenfolge:

1. Erste Regelgruppen, von Ihnen in der Firewall Manager Manager-DNS-Firewall-Richtlinie definiert. Gültige Werte liegen zwischen 1 und 99.
2. DNS-Firewall-Regelgruppen, die von einzelnen Kontomanagern über die DNS-Firewall zugeordnet werden.
3. Letzte Regelgruppen, von Ihnen in der Firewall Manager Manager-DNS-Firewall-Richtlinie definiert. Gültige Werte liegen zwischen 9901 und 10000.

Löschen einer Regelgruppe

Um eine Regelgruppe aus einer Firewall Manager Manager-DNS-Firewall-Richtlinie zu löschen, müssen Sie die folgenden Schritte ausführen:

1. Entfernen Sie die Regelgruppe aus Ihrer Firewall Manager Manager-DNS-Firewall-Richtlinie.
2. Heben Sie die gemeinsame Nutzung der Regelgruppe in auf AWS Resource Access Manager. Um die gemeinsame Nutzung einer Regelgruppe, deren Eigentümer Sie sind, rückgängig zu machen, müssen Sie sie aus der Ressourcenfreigabe entfernen. Sie können dies über die AWS RAM Konsole oder die AWS CLI tun. Informationen zum Aufheben der gemeinsamen Nutzung einer Ressource finden Sie unter [Aktualisieren einer Ressourcenfreigabe AWS RAM im AWS RAM Benutzerhandbuch](#).
3. Löschen Sie die Regelgruppe mithilfe der DNS-Firewall-Konsole oder AWS CLI.

So benennt Firewall Manager die von ihm erstellten Regelgruppenzuordnungen

Wenn Sie die DNS-Firewallrichtlinie speichern und die automatische Behebung aktiviert haben, erstellt Firewall Manager eine DNS-Firewall-Zuordnung zwischen den Regelgruppen, die Sie in der Richtlinie angegeben haben, und den VPCs, die in den Geltungsbereich der Richtlinie fallen. Firewall Manager benennt diese Zuordnungen, indem er die folgenden Werte verkettet:

- Die feste Zeichenfolge, . FMManaged_

- Die Firewall Manager Manager-Richtlinien-ID. Dies ist die AWS Ressourcen-ID für die Firewall Manager Manager-Richtlinie.

Im Folgenden sehen Sie einen Beispielnamen für eine Firewall, die von Firewall Manager verwaltet wird:

```
FManaged_EXAMPLEDNSFirewallPolicyId
```

Wenn Kontoinhaber in den VPCs nach der Erstellung der Richtlinie Ihre Firewall-Richtlinieneinstellungen oder Ihre Regelgruppenzuordnungen überschreiben, markiert Firewall Manager die Richtlinie als nicht konform und versucht, eine Abhilfemaßnahme vorzuschlagen. Kontoinhaber können den VPCs, die in den Geltungsbereich der DNS-Firewall-Richtlinie fallen, andere DNS-Firewall-Regelgruppen zuordnen. Für alle Verknüpfungen, die von den einzelnen Kontoinhabern erstellt werden, müssen Prioritätseinstellungen zwischen Ihrer ersten und letzten Regelgruppenverknüpfung festgelegt werden.

NGFW-Richtlinien für die Cloud von Palo Alto Networks

Die Palo Alto Networks Cloud Next Generation Firewall (NGFW) ist ein Firewall-Service eines Drittanbieters, den Sie für Ihre Richtlinien verwenden können. AWS Firewall Manager Mit Palo Alto Networks Cloud NGFW for Firewall Manager können Sie Palo Alto Networks Cloud NGFW-Ressourcen und Regelstapel für all Ihre Konten erstellen und zentral bereitstellen. AWS

Um Palo Alto Networks Cloud NGFW mit Firewall Manager zu verwenden, abonnieren Sie zunächst den [Palo Alto Networks Cloud NGFW](#) Pay-As-You-Go-Dienst im Marketplace. AWS Nach dem Abonnement führen Sie im Palo Alto Networks Cloud NGFW-Dienst eine Reihe von Schritten aus, um Ihr Konto und Ihre Cloud NGFW-Einstellungen zu konfigurieren. Anschließend erstellen Sie eine Firewall Manager Cloud FMS-Richtlinie, um Palo Alto Networks Cloud NGFW-Ressourcen und -Regeln für alle Konten in Ihren Organizations zentral bereitzustellen und zu verwalten. AWS

Das Verfahren zum Erstellen der Firewall Manager Manager-Richtlinie finden Sie unter [Eine AWS Firewall Manager Richtlinie für Palo Alto Networks Cloud NGFW erstellen](#). Informationen zur Konfiguration und Verwaltung von Palo Alto Networks Cloud NGFW für Firewall Manager finden Sie in der Dokumentation [Palo Alto Networks Cloud NGFW von Palo Alto Networks](#). AWS

Richtlinien für die Fortigate Cloud Native Firewall (CNF) als Service

Fortigate Cloud Native Firewall (CNF) as a Service ist ein Firewall-Service eines Drittanbieters, den Sie für Ihre Richtlinien verwenden können. AWS Firewall Manager Fortigate CNF ist ein Firewall-

Service der nächsten Generation, der es Ihnen leicht macht, Ihre Cloud-Netzwerke zu schützen und Ihre Sicherheitsrichtlinien zu verwalten. Mit Fortigate CNF for Firewall Manager können Sie Fortigate CNF-Ressourcen und Richtlinienätze für all Ihre Konten erstellen und zentral bereitstellen. AWS

Um Fortigate CNF mit Firewall Manager zu verwenden, abonnieren Sie zunächst die [Fortigate Cloud Native Firewall \(CNF\) as a Service](#) im Marketplace. AWS Nach dem Abonnement führen Sie eine Reihe von Schritten im Fortigate CNF-Service durch, um Ihre globalen Richtlinienätze und andere Einstellungen zu konfigurieren. Anschließend erstellen Sie eine Firewall Manager Manager-Richtlinie, um Fortigate CNF-Ressourcen für alle Konten in Ihren Organizations zentral bereitzustellen und zu verwalten. AWS

Das Verfahren zum Erstellen einer Fortigate CNF Firewall Manager Manager-Richtlinie finden Sie unter [Erstellen einer AWS Firewall Manager Richtlinie für Fortigate Cloud Native Firewall \(CNF\) as a Service](#) Informationen zur Konfiguration und Verwaltung von Fortigate CNF für die Verwendung mit Firewall Manager finden Sie in der [Fortigate](#) CNF-Dokumentation.

Gemeinsame Nutzung von Ressourcen für Network Firewall- und DNS-Firewall-Richtlinien

Um die Netzwerkfirewall- und DNS-Firewall-Richtlinien von Firewall Manager zu verwalten, müssen Sie die gemeinsame Nutzung von Ressourcen mit AWS Organizations in aktivieren AWS Resource Access Manager. Auf diese Weise kann Firewall Manager Schutzmaßnahmen für Ihre Konten bereitstellen, wenn Sie diese Richtlinientypen erstellen.

Um die gemeinsame Nutzung von Ressourcen zu aktivieren, folgen Sie den Anweisungen unter [Gemeinsame Nutzung aktivieren mit AWS Organizations](#) im AWS Resource Access Manager Benutzerhandbuch.

Probleme mit der gemeinsamen Nutzung von Ressourcen

Möglicherweise treten Probleme mit der gemeinsamen Nutzung von Ressourcen auf, entweder wenn Sie sie aktivieren oder wenn Sie an Firewall Manager Manager-Richtlinien arbeiten, die dies erfordern. AWS RAM

Zu diesen Problemen gehören beispielsweise die folgenden:

- Wenn Sie den Anweisungen zum Aktivieren der Freigabe folgen, AWS Organizations ist die Option Teilen aktivieren in der AWS RAM Konsole ausgegraut und steht nicht zur Auswahl.
- Wenn Sie in Firewall Manager an einer Richtlinie arbeiten, die die gemeinsame Nutzung von Ressourcen erfordert, wird die Richtlinie als nicht konform markiert und es werden Meldungen

angezeigt, die darauf hinweisen, dass die gemeinsame Nutzung von Ressourcen aktiviert AWS RAM ist oder nicht aktiviert ist.

Wenn Sie Probleme mit der gemeinsamen Nutzung von Ressourcen haben, versuchen Sie mit dem folgenden Verfahren, sie zu aktivieren.

Versuchen Sie erneut, die gemeinsame Nutzung von Ressourcen zu aktivieren

- Versuchen Sie erneut, die gemeinsame Nutzung mit einer der folgenden Optionen zu aktivieren:
 - (Option) Folgen Sie über die AWS RAM Konsole den Anweisungen unter [Teilen aktivieren mit AWS Organizations](#) im AWS Resource Access Manager Benutzerhandbuch.
 - (Option) Rufen Sie über die AWS RAM API auf `EnableSharingWithAwsOrganization`. Die Dokumentation finden Sie unter [EnableSharingWithAwsOrganization](#).

Arbeiten mit Ressourcensätzen in Firewall Manager

Ein AWS Firewall Manager Ressourcensatz ist eine Sammlung von Ressourcen, z. B. Firewalls, die Sie in einer Firewall Manager Manager-Richtlinie gruppieren und verwalten können. Mithilfe von Ressourcensätzen können Mitglieder in Ihrer Organisation detailliert steuern, welche Ressourcen in einer Richtlinie verwaltet werden sollen. Um Ressourcensätze zu verwenden, erstellen Sie einen Ressourcensatz in der Konsole oder mithilfe der [PutResourceSetAPI](#) und fügen Sie den Ressourcensatz dann zu Ihrer Firewall Manager Manager-Richtlinie hinzu.

Sie können Ressourcensätze für die folgenden Ressourcen- und Sicherheitsrichtlinientypen erstellen und verwalten:

Ressourcentyp	Sicherheitsrichtlinientyp für Firewall Manager
AWS Network Firewall - Firewalls	Netzwerk-Firewall-Richtlinie — Verwenden Sie Ressourcensätze, um bestehende Firewalls aus der Network Firewall zu importieren. Informationen zur Verwendung von Ressourcensätzen in einer Netzwerk-Firewall-Richtlinie finden Sie im Verfahrensschritt Importieren vorhandener Firewalls . Eine AWS Firewall Manager Richtlinie erstellen für AWS Network Firewall

In den folgenden Abschnitten werden die Anforderungen für das Erstellen und Löschen von Ressourcensätzen behandelt.

Themen

- [Überlegungen bei der Arbeit mit Ressourcensätzen in Firewall Manager](#)
- [Ressourcensets erstellen](#)
- [Löschen eines Ressourcensatzes](#)

Überlegungen bei der Arbeit mit Ressourcensätzen in Firewall Manager

Beachten Sie bei der Arbeit mit Ressourcensätzen die folgenden Überlegungen

Verweise auf nicht existierende Ressourcen

Wenn Sie einer Ressourcengruppe eine Ressource hinzufügen, erstellen Sie mithilfe eines Amazon-Ressourcennamens (ARN) einen Verweis auf die Ressource. Firewall Manager überprüft, ob Amazon Resource Name (ARN) das richtige Format hat, aber Firewall Manager überprüft nicht, ob die referenzierte Ressource existiert. Wenn die Ressource noch nicht existiert und die ARN-Validierung bestanden hat, nimmt Firewall Manager die Ressourcenreferenz in die Ressourcengruppe auf. Wenn später eine neue Ressource mit demselben ARN erstellt wird, wendet Firewall Manager Regelgruppen aus der mit dem Ressourcensatz verknüpften Richtlinie auf die neue Ressource an.

Gelöschte Ressourcen

Wenn eine Ressource in einem Ressourcensatz gelöscht wird, verbleibt der Verweis auf die Ressource in der Ressourcengruppe, bis er vom Firewall Manager Manager-Administrator entfernt wird.

Ressourcen, die einem Mitgliedskonto gehören, das die AWS Organizations Organisation verlässt

Wenn ein Mitgliedskonto die Organisation verlässt, verbleiben alle Verweise auf Ressourcen, die diesem Mitgliedskonto gehören, in der Ressourcengruppe, werden aber nicht mehr durch Richtlinien verwaltet, mit denen die Ressourcengruppe verknüpft ist.


Zuordnung zu mehreren Richtlinien

Ein Ressourcensatz kann mehreren Richtlinien zugeordnet werden, aber nicht alle Richtlinientypen unterstützen mehrere Richtlinien, die dieselbe Ressource verwalten. Informationen zu nicht unterstützten Szenarien finden Sie in der Dokumentation für Ihren spezifischen Richtlinientyp.

Ressourcensets erstellen

Um einen Ressourcensatz zu erstellen (Konsole)

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

 Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Resource Sets aus.
3. Wählen Sie Ressourcensatz erstellen aus.
4. Geben Sie unter Name des Ressourcensatzes einen aussagekräftigen Namen ein.
5. (Optional) Geben Sie eine Beschreibung für den Ressourcensatz ein.
6. Wählen Sie Weiter aus.
7. Wählen Sie unter Ressourcen auswählen eine AWS Konto-ID und anschließend Ressourcen auswählen aus, um Ressourcen, die diesem Konto gehören und von diesem Konto verwaltet werden, dem Ressourcensatz hinzuzufügen. Nachdem Sie die Ressourcen ausgewählt haben, wählen Sie Hinzufügen aus, um die Ressourcen dem Ressourcensatz hinzuzufügen.
8. Wählen Sie Weiter aus.
9. Fügen Sie unter Ressourcensatz-Tags alle identifizierenden Tags hinzu, die Sie für den Ressourcensatz benötigen. Weitere Informationen zu Tags finden Sie unter [Arbeiten mit dem Tag Editor](#).
10. Wählen Sie Weiter aus.
11. Prüfen Sie den neuen Ressourcensatz. Um Änderungen vorzunehmen, wählen Sie Edit (Bearbeiten) in dem Bereich, den Sie ändern möchten. Dadurch kehren Sie zum entsprechenden Schritt im Erstellungsassistenten zurück. Wenn Sie mit dem Ressourcensatz zufrieden sind, wählen Sie Create Resource Set aus.

Löschen eines Ressourcensatzes

Bevor Sie einen Ressourcensatz löschen können, muss der Ressourcensatz von allen Richtlinien getrennt werden, die den Ressourcensatz verwenden. Sie können die Zuordnung von Ressourcengruppen auf der Seite mit den Richtlinienetails mithilfe der Konsole oder mit der [PutPolicy](#)API aufheben.

Um einen Ressourcensatz zu löschen (Konsole)

1. Wählen Sie im Navigationsbereich Resource Sets aus.

2. Wählen Sie die Option neben dem Ressourcensatz aus, den Sie löschen möchten.
3. Wählen Sie Löschen.

Compliance-Informationen für eine AWS Firewall Manager Richtlinie anzeigen

Dieser Abschnitt enthält Anleitungen zur Anzeige des Konformitätsstatus von Konten und Ressourcen, die in den Geltungsbereich einer AWS Firewall Manager Richtlinie fallen. Informationen zu den Kontrollen, die unter AWS zur Aufrechterhaltung der Sicherheit und Einhaltung von Vorschriften in der Cloud eingerichtet wurden, finden Sie unter [Konformitätsprüfung für Firewall Manager](#).

Note

Damit Firewall Manager die Einhaltung der Richtlinien überwachen kann, AWS Config müssen die Konfigurationsänderungen für geschützte Ressourcen kontinuierlich aufgezeichnet werden. In Ihrer AWS Config Konfiguration muss die Aufzeichnungsfrequenz auf Kontinuierlich eingestellt sein, was die Standardeinstellung ist.

Note


Um den ordnungsgemäßen Compliance-Status Ihrer geschützten Ressourcen aufrechtzuerhalten, sollten Sie es vermeiden, den Status der Firewall Manager Manager-Schutzmaßnahmen wiederholt zu ändern, entweder automatisch oder manuell. Firewall Manager verwendet Informationen von AWS Config , um Änderungen an Ressourcenkonfigurationen zu erkennen. Wenn Änderungen schnell genug angewendet werden, AWS Config kann der Überblick über einige Änderungen verloren gehen, was zum Verlust von Informationen über den Konformitäts- oder Behebungsstatus in Firewall Manager führen kann.

Wenn Sie feststellen, dass eine Ressource, die Sie mit Firewall Manager schützen, einen falschen Konformitäts- oder Behebungsstatus hat, stellen Sie zunächst sicher, dass Sie keinen Prozess ausführen, der Ihren Firewall Manager Manager-Schutz ändert oder zurücksetzt, und aktualisieren Sie dann das AWS Config Tracking für die Ressource, indem Sie die zugehörigen Konfigurationsregeln unter neu bewerten. AWS Config

Für alle AWS Firewall Manager Richtlinien können Sie den Konformitätsstatus der Konten und Ressourcen einsehen, die in den Geltungsbereich der Richtlinie fallen. Ein Konto oder eine Ressource entspricht einer Firewall Manager Manager-Richtlinie, wenn sich die Einstellungen in der Richtlinie in den Einstellungen für das Konto oder die Ressource widerspiegeln. Jeder Richtlinientyp hat seine eigenen Compliance-Anforderungen, die Sie bei der Definition der Richtlinie anpassen können. Bei einigen Richtlinien können Sie auch detaillierte Informationen zu Verstößen für in den jeweiligen Anwendungsbereich fallende Ressourcen einsehen, damit Sie Ihr Sicherheitsrisiko besser verstehen und steuern können.

Um die Compliance-Informationen für eine Richtlinie einzusehen

1. Melden Sie sich AWS Management Console mit Ihrem Firewall Manager Manager-Administratorkonto an und öffnen Sie dann die Firewall Manager Manager-Konsole unter <https://console.aws.amazon.com/wafv2/fmsv2>. Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

 Note

Weitere Informationen zum Einrichten eines Firewall Manager-Administratorkontos finden Sie unter [AWS Firewall Manager Voraussetzungen](#).

2. Wählen Sie im Navigationsbereich Security policies (Sicherheitsrichtlinien) aus.
3. Wählen Sie eine Richtlinie aus. Auf der Registerkarte Konten und Ressourcen der Richtlinienseite listet Firewall Manager die Konten in Ihrer Organisation auf, gruppiert nach Konten, die innerhalb des Geltungsbereichs der Richtlinie liegen, und Konten, die außerhalb des Geltungsbereichs liegen.

Im Bereich Konten im Geltungsbereich der Richtlinie wird der Konformitätsstatus für jedes Konto aufgeführt. Der Status „Konform“ bedeutet, dass die Richtlinie erfolgreich auf alle Ressourcen des Kontos angewendet wurde, die in den Geltungsbereich fallen. Der Status Nicht konform bedeutet, dass die Richtlinie nicht auf eine oder mehrere Ressourcen angewendet wurde, die in den Geltungsbereich des Kontos fallen.

4. Wählen Sie ein Konto aus, das nicht konform ist. Auf der Kontoseite listet Firewall Manager die ID und den Typ für jede nicht konforme Ressource sowie den Grund für den Verstoß der Ressource gegen die Richtlinie auf.

Note

Für die Ressourcentypen `AWS::EC2::NetworkInterface` (ENI) und `AWS::EC2::Instance` zeigt Firewall Manager möglicherweise eine begrenzte Anzahl nicht konformer Ressourcen an. Um weitere nicht konforme Ressourcen aufzulisten, korrigieren Sie die Ressourcen, die ursprünglich für das Konto angezeigt wurden.

5. Wenn der Firewall Manager Manager-Richtlinientyp eine Inhaltsüberwachungs-Sicherheitsgruppenrichtlinie ist, können Sie auf detaillierte Informationen zu Verstößen für eine Ressource zugreifen.

Um Details zum Verstoß anzuzeigen, wählen Sie die Ressource aus.

Note

Ressourcen, die Firewall Manager vor dem Hinzufügen der detaillierten Seite mit den Ressourcenverstößen für nicht konform befunden hat, enthalten möglicherweise keine Verstoßdetails.

Auf der Ressourcenseite listet Firewall Manager je nach Ressourcentyp spezifische Details zu der Verletzung auf.

- **AWS::EC2::NetworkInterface**(ENI) — Firewall Manager zeigt Informationen über die Sicherheitsgruppe an, der die Ressource nicht entspricht. Wählen Sie die Sicherheitsgruppe aus, um weitere Informationen dazu zu erhalten.
- **AWS::EC2::Instance**— Firewall Manager zeigt die ENI an, die an die EC2-Instance angehängt ist und die nicht konform ist. Außerdem werden Informationen über die Sicherheitsgruppe angezeigt, der die Ressourcen nicht entsprechen. Wählen Sie die Sicherheitsgruppe aus, um weitere Informationen dazu zu erhalten.
- **AWS::EC2::SecurityGroup**— Firewall Manager zeigt die folgenden Verstoßdetails an:
 - Nichtkonforme Sicherheitsgruppenregel — Die Regel, gegen die verstoßen wurde, einschließlich Protokoll, Portbereich, IP-CIDR-Bereich und Beschreibung.
 - Referenzierte Regel — Die Audit-Sicherheitsgruppenregel, gegen die die nichtkonforme Sicherheitsgruppenregel verstößt, mit ihren Einzelheiten.
 - Gründe für den Verstoß — Erläuterung des festgestellten Verstoßes.

- Abhilfemaßnahme — Vorgeschlagene Maßnahme. Wenn Firewall Manager keine sichere Behebungsaktion ermitteln kann, ist dieses Feld leer.
- **AWS::EC2::Subnet** — Dies wird für Netzwerk-Firewall-Richtlinien verwendet. Firewall Manager zeigt die Subnetz-ID, VPC-ID und Availability Zone an. Falls zutreffend, enthält Firewall Manager zusätzliche Informationen über den Verstoß, z. B. den Grund des Verstoßes oder die ID der Routing-Tabelle, mit der ein Subnetz verknüpft werden soll. Die Komponente zur Beschreibung des Verstoßes enthält eine Beschreibung des erwarteten Zustands der Ressource, des aktuellen Status, der nicht konform ist, und, falls verfügbar, eine Beschreibung der Ursache der Diskrepanz.

Der erwartete Status eines Subnetzes könnte beispielsweise „Das Subnetz sollte ein AWS Network Firewall Subnetz in seiner Availability Zone enthalten“ lauten, der aktuelle Status könnte lauten „Subnetz mit der ID subnet-1234 fehlt ein Network Firewall Firewall-Subnetz in der Availability Zone us-east-1e“ und die Beschreibung könnte lauten: „Firewall Manager konnte in dieser AZ kein Subnetz erstellen, weil keine CIDR-Blöcke verfügbar sind“.

- Verstöße gegen die Routenverwaltung — Für Netzwerk-Firewall-Richtlinien, die den Überwachungsmodus verwenden, zeigt Firewall Manager grundlegende Subnetzinformationen sowie erwartete und tatsächliche Routen in der Subnetz-, Internet-Gateway- und Netzwerkfirewall-Subnetz-Routentabelle an. Firewall Manager warnt Sie, dass ein Verstoß vorliegt, wenn die tatsächlichen Routen nicht mit den erwarteten Routen in der Routentabelle übereinstimmen.
- Behebungsmaßnahmen für Verstöße gegen die Routenverwaltung — Für Netzwerk-Firewall-Richtlinien, die den Überwachungsmodus verwenden, schlägt Firewall Manager mögliche Behebungsmaßnahmen für Routenkonfigurationen vor, die Verstöße aufweisen.

Example — Verstöße gegen die Routenverwaltung und Vorschläge zur Behebung

Es wird erwartet, dass ein Subnetz Datenverkehr über die Firewall-Endpunkte sendet, aber das aktuelle Subnetz sendet den Verkehr direkt an das Internet-Gateway. Dies ist ein Verstoß gegen die Routenverwaltung. Die vorgeschlagene Abhilfe könnte in diesem Fall eine Liste angeordneter Aktionen sein. Die erste ist eine Empfehlung, die erforderlichen Routen zur Routentabelle des Netzwerkfirewall-Subnetzes hinzuzufügen, um ausgehenden Verkehr an das Internet-Gateway und um eingehenden Verkehr für Ziele innerhalb der VPC weiterzuleiten. Die zweite Empfehlung besteht darin, die Internet-Gateway-Route oder die ungültige Netzwerk-Firewall-Route in der Routing-Tabelle des Subnetzes zu ersetzen, um ausgehenden Verkehr an die Firewall-Endpunkte weiterzuleiten. Die dritte Empfehlung besteht darin,

die erforderlichen Routen zur Routing-Tabelle des Internet-Gateways hinzuzufügen, um eingehenden Verkehr an die Firewall-Endpunkte weiterzuleiten.

- **AWS::EC2:InternetGateway**— Dies wird für Netzwerk-Firewall-Richtlinien verwendet, für die der Überwachungsmodus aktiviert ist.
 - Verstöße gegen die Routenverwaltung — Das Internet-Gateway ist nicht konform, wenn das Internet-Gateway keiner Routing-Tabelle zugeordnet ist oder wenn die Internet-Gateway-Routentabelle eine ungültige Route enthält.
 - Behebungsmaßnahmen bei Verstößen gegen die Routenverwaltung — Firewall Manager schlägt mögliche Behebungsmaßnahmen vor, um Verstöße gegen die Routenverwaltung zu beheben.

Example 1 — Verstöße gegen die Routenverwaltung und Vorschläge zur Behebung

Ein Internet-Gateway ist keiner Routing-Tabelle zugeordnet. Bei den vorgeschlagenen Behebungsmaßnahmen kann es sich um eine Liste geordneter Aktionen handeln. Die erste Aktion besteht darin, eine Routentabelle zu erstellen. Die zweite Aktion besteht darin, die Routing-Tabelle dem Internet-Gateway zuzuordnen. Die dritte Aktion besteht darin, die erforderliche Route zur Internet-Gateway-Routentabelle hinzuzufügen.

Example 2 — Verstöße gegen das Routenmanagement und Vorschläge zur Behebung

Das Internet-Gateway ist mit einer gültigen Routing-Tabelle verknüpft, aber die Route ist falsch konfiguriert. Bei der vorgeschlagenen Abhilfemaßnahme könnte es sich um eine Liste angeordneter Aktionen handeln. Der erste Vorschlag besteht darin, die ungültige Route zu entfernen. Die zweite Möglichkeit besteht darin, die erforderliche Route zur Internet-Gateway-Routentabelle hinzuzufügen.

- **AWS::NetworkFirewall::FirewallPolicy**— Dies wird für Netzwerk-Firewall-Richtlinien verwendet. Firewall Manager zeigt Informationen über eine Netzwerk-Firewall-Richtlinie an, die so geändert wurde, dass sie nicht mehr konform ist. Die Informationen enthalten die erwartete Firewall-Richtlinie und die Richtlinie, die sie im Kundenkonto gefunden hat, sodass Sie die Namen und Prioritätseinstellungen für statusfreie und statusbehaftete Regelgruppen, benutzerdefinierte Aktionsnamen und Standardeinstellungen für statusfreie Aktionen vergleichen können. Die Komponente zur Beschreibung des Verstoßes enthält eine Beschreibung des erwarteten Zustands der Ressource, des aktuellen Status, der nicht konform ist, und, falls verfügbar, eine Beschreibung der Ursache der Diskrepanz.
- **AWS::EC2::VPC**— Dies wird für DNS-Firewall-Richtlinien verwendet. Firewall Manager zeigt Informationen über eine VPC an, die in den Geltungsbereich einer Firewall Manager Manager-

DNS-Firewall-Richtlinie fällt und die nicht mit der Richtlinie konform ist. Die bereitgestellten Informationen umfassen die erwarteten Regelgruppen, die voraussichtlich der VPC zugeordnet werden, und die tatsächlichen Regelgruppen. Die Komponente zur Beschreibung des Verstoßes enthält eine Beschreibung des erwarteten Zustands der Ressource, des aktuellen Status, der nicht konform ist, und, falls verfügbar, eine Beschreibung der Ursache der Diskrepanz.

AWS Firewall Manager Befunde

AWS Firewall Manager erstellt Ergebnisse für Ressourcen, die nicht richtlinientreu sind, sowie für erkannte Angriffe und sendet sie an diese weiter AWS Security Hub. Informationen zu den Ergebnissen von Security Hub finden Sie unter [Ergebnisse in AWS Security Hub](#).

Wenn Sie Security Hub und Firewall Manager verwenden, sendet Firewall Manager Ihre Ergebnisse automatisch an Security Hub. Informationen zu den ersten Schritten mit Security Hub finden Sie unter [Einrichtung AWS Security Hub](#) im [AWS Security Hub Benutzerhandbuch](#).

Wie kann ich meine Firewall Manager Manager-Ergebnisse einsehen?

Um Ihre Firewall Manager Manager-Ergebnisse in Security Hub anzuzeigen, folgen Sie den Anweisungen unter [Arbeiten mit Ergebnissen in Security Hub](#) und erstellen Sie einen Filter mit den folgenden Einstellungen:

- Attribut auf Product name (Produktname) gesetzt.
- Operator auf EQUALS (GLEICH) gesetzt.
- Wert auf Firewall Manager gesetzt. Bei dieser Einstellung wird die Groß- und Kleinschreibung unterschieden.

Kann ich dies deaktivieren?

Sie können die Integration von AWS Firewall Manager Ergebnissen mit Security Hub über die Security Hub Hub-Konsole deaktivieren. Wählen Sie in der Navigationsleiste Integrationen und dann im Bereich Firewall Manager die Option Integration deaktivieren aus. Weitere Informationen finden Sie im [AWS Security Hub -Benutzerhandbuch](#).

AWS Firewall Manager Typen finden

- [AWS WAF politische Ergebnisse](#)

- [AWS Shield Advanced politische Feststellungen](#)
- [Allgemeine Richtlinienkenntnisse der Sicherheitsgruppe](#)
- [Erkenntnisse der Prüfungsrichtlinie für Sicherheitsgruppen](#)
- [Erkenntnisse der Überwachungsrichtlinie für Sicherheitsgruppen](#)
- [Ergebnisse der Amazon Route 53 Resolver DNS-Firewall-Richtlinie](#)

AWS WAF politische Ergebnisse

Sie können die AWS WAF Richtlinien von Firewall Manager verwenden, um AWS WAF Regelgruppen auf Ihre Ressourcen in anzuwenden AWS Organizations. Weitere Informationen finden Sie unter [Mit AWS Firewall Manager Richtlinien arbeiten](#).

Der Ressource fehlt die von Firewall Manager verwaltete Web-ACL.

Eine AWS Ressource verfügt nicht über die AWS Firewall Manager verwaltete Web-ACL-Zuordnung gemäß der Firewall Manager Manager-Richtlinie. Sie können die Firewall Manager Manager-Wiederherstellung für die Richtlinie aktivieren, um dies zu korrigieren.

- Schweregrad — 80
- Stauseinstellungen — BESTANDEN/FEHLGESCHLAGEN
- Updates — Wenn Firewall Manager die Behebungsaktion durchführt, aktualisiert er das Ergebnis und der Schweregrad wird von HIGH bis INFORMATIONAL herabgesetzt. Wenn Sie die Wiederherstellung durchführen, aktualisiert Firewall Manager das Ergebnis nicht.

Die von Firewall Manager verwaltete Web-ACL hat falsch konfigurierte Regelgruppen.

Die Regelgruppen in einer Web-ACL, die von Firewall Manager verwaltet wird, sind gemäß der Firewall Manager Manager-Richtlinie nicht korrekt konfiguriert. Dies bedeutet, dass der Web-ACL die Regelgruppen fehlen, die von der Richtlinie benötigt werden. Sie können die Firewall Manager Manager-Wiederherstellung für die Richtlinie aktivieren, um dies zu korrigieren.

- Schweregrad — 80
- Stauseinstellungen — BESTANDEN/FEHLGESCHLAGEN
- Updates — Wenn Firewall Manager die Behebungsaktion durchführt, aktualisiert er das Ergebnis und der Schweregrad wird von HIGH bis INFORMATIONAL herabgesetzt. Wenn Sie die Wiederherstellung durchführen, aktualisiert Firewall Manager das Ergebnis nicht.

AWS Shield Advanced politische Feststellungen

Informationen zu AWS Shield Advanced Richtlinien finden Sie unter [Sicherheitsgruppenrichtlinien](#).

Der Ressource fehlt der Shield Advanced-Schutz.

Eine AWS Ressource, die gemäß der Firewall Manager Manager-Richtlinie über Shield Advanced-Schutz verfügen sollte, hat diesen nicht. Sie können die Firewall Manager Manager-Wiederherstellung für die Richtlinie aktivieren, wodurch der Schutz für die Ressource aktiviert wird.

- Schweregrad — 60
- Stauseinstellungen — BESTANDEN/FEHLGESCHLAGEN
- Updates — Wenn Firewall Manager die Behebungsaktion durchführt, aktualisiert er das Ergebnis und der Schweregrad wird von HIGH bis INFORMATIONAL herabgesetzt. Wenn Sie die Wiederherstellung durchführen, aktualisiert Firewall Manager das Ergebnis nicht.

Shield Advanced hat einen Angriff auf die überwachte Ressource erkannt.

Shield Advanced hat einen Angriff auf eine geschützte AWS Ressource erkannt. Sie können die Firewall Manager Manager-Wiederherstellung für die Richtlinie aktivieren.

- Schweregrad — 70
- Stauseinstellungen — Keine
- Updates — Firewall Manager aktualisiert dieses Ergebnis nicht.

Allgemeine Richtlinienerkenntnisse der Sicherheitsgruppe

Hinweise zu allgemeinen Richtlinien für Sicherheitsgruppen finden Sie unter [Sicherheitsgruppenrichtlinien](#).

Die Ressource hat die Sicherheitsgruppe falsch konfiguriert.

Firewall Manager hat eine Ressource identifiziert, der die von Firewall Manager verwalteten Sicherheitsgruppenzuordnungen fehlen, die sie gemäß der Firewall Manager Manager-Richtlinie haben sollte. Sie können die Firewall Manager Manager-Wiederherstellung für die Richtlinie aktivieren, wodurch die Verknüpfungen gemäß den Richtlinieneinstellungen erstellt werden.

- Schweregrad — 70

- Stuseinstellungen — BESTANDEN/FEHLGESCHLAGEN
- Updates — Firewall Manager aktualisiert dieses Ergebnis.

Die Firewall Manager Manager-Replikatsicherheitsgruppe ist nicht mit der primären Sicherheitsgruppe synchronisiert.

Eine Firewall Manager Manager-Replikatsicherheitsgruppe ist gemäß ihrer gemeinsamen Sicherheitsgruppenrichtlinie nicht mit ihrer primären Sicherheitsgruppe synchron. Sie können die Firewall Manager Manager-Wiederherstellung für die Richtlinie aktivieren, wodurch die Replikatsicherheitsgruppen mit der primären synchronisiert werden.

- Schweregrad — 80
- Stuseinstellungen — BESTANDEN/FEHLGESCHLAGEN
- Updates — Firewall Manager aktualisiert dieses Ergebnis.

Erkenntnisse der Prüfungsrichtlinie für Sicherheitsgruppen

Hinweise zu Sicherheitsgruppen-Inhaltsprüfungsrichtlinien finden Sie unter [Sicherheitsgruppenrichtlinien](#).

Es besteht keine Compliance zwischen Sicherheitsgruppe und Inhaltsprüfungssicherheitsgruppe.

Eine Inhaltsüberwachungsrichtlinie von Firewall Manager für Sicherheitsgruppen hat eine nicht konforme Sicherheitsgruppe identifiziert. Dies ist eine vom Kunden erstellte Sicherheitsgruppe, die sich im Bereich der Inhaltsprüfungsrichtlinie befindet, und die nicht mit den Einstellungen übereinstimmt, die von der Richtlinie und ihrer Prüfungssicherheitsgruppe definiert werden. Sie können die Firewall Manager Manager-Wiederherstellung für die Richtlinie aktivieren, wodurch die nicht konforme Sicherheitsgruppe geändert wird, um sie konform zu machen.

- Schweregrad — 70
- Stuseinstellungen — BESTANDEN/FEHLGESCHLAGEN
- Updates — Firewall Manager aktualisiert dieses Ergebnis.

Erkenntnisse der Überwachungsrichtlinie für Sicherheitsgruppen

Hinweise zu Überwachungsrichtlinien für die Verwendung von Sicherheitsgruppen finden Sie unter [Sicherheitsgruppenrichtlinien](#).

Firewall Manager hat eine redundante Sicherheitsgruppe gefunden.

Das Audit zur Nutzung der Firewall Manager Manager-Sicherheitsgruppe hat eine redundante Sicherheitsgruppe identifiziert. Dies ist eine Sicherheitsgruppe mit identischen Regeln wie eine andere Sicherheitsgruppe innerhalb derselben Amazon Virtual Private Cloud Cloud-Instance. Sie können die automatische Wiederherstellung von Firewall Manager für die Nutzungsüberwachungsrichtlinie aktivieren, wodurch redundante Sicherheitsgruppen ersetzt werden, und zwar durch eine einzige Sicherheitsgruppe.

- Schweregrad — 30
- Stauseinstellungen — Keine
- Updates — Firewall Manager aktualisiert dieses Ergebnis nicht.

Der Firewall Manager hat eine unbenutzte Sicherheitsgruppe gefunden.

Das Audit zur Nutzung der Firewall Manager Manager-Sicherheitsgruppe hat eine ungenutzte Sicherheitsgruppe identifiziert. Dies ist eine Sicherheitsgruppe, auf die in keiner allgemeinen Sicherheitsgruppenrichtlinie von Firewall Manager verwiesen wird. Sie können die automatische Wiederherstellung von Firewall Manager für die Nutzungsüberwachungsrichtlinie aktivieren, wodurch nicht verwendete Sicherheitsgruppen entfernt werden.

- Schweregrad — 30
- Stauseinstellungen — Keine
- Updates — Firewall Manager aktualisiert dieses Ergebnis nicht.

Ergebnisse der Amazon Route 53 Resolver DNS-Firewall-Richtlinie

Informationen zu DNS-Firewall-Richtlinien finden Sie unter [DNS-Firewall-Richtlinien für Amazon Route 53 Resolver](#).

Der Ressource fehlt der DNS-Firewall-Schutz

In einer VPC fehlt eine DNS-Firewall-Regelgruppenzuordnung, die in der DNS-Firewall-Richtlinie von Firewall Manager definiert ist. Das Ergebnis listet die Regelgruppe auf, die in der Richtlinie angegeben ist.

- Schweregrad — 80

Sicherheit in AWS Firewall Manager

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Die Wirksamkeit unserer Sicherheitsfunktionen wird regelmäßig von externen Prüfern im Rahmen des [AWS -Compliance-Programms getestet und überprüft](#). Informationen zu den Compliance-Programmen, die für Firewall Manager gelten, finden Sie unter [AWS Services in Scope by Compliance Program](#).
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. In Ihre Verantwortung fallen außerdem weitere Faktoren, wie z. B. die Vertraulichkeit der Daten, die Anforderungen Ihrer Organisation sowie geltende Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Firewall Manager anwenden können. In den folgenden Themen erfahren Sie, wie Sie Firewall Manager so konfigurieren, dass Sie Ihre Sicherheits- und Compliance-Ziele erreichen. Sie erfahren auch, wie Sie andere AWS Dienste verwenden können, mit denen Sie Ihre Firewall Manager Manager-Ressourcen überwachen und sichern können.

Themen

- [Datenschutz im Firewall Manager](#)
- [Identity and Access Management für AWS Firewall Manager](#)
- [Protokollierung und Überwachung in Firewall Manager](#)
- [Konformitätsprüfung für Firewall Manager](#)
- [Resilienz im Firewall Manager](#)
- [Sicherheit der Infrastruktur in AWS Firewall Manager](#)

Datenschutz im Firewall Manager

Das [Modell der AWS gemeinsamen Verantwortung](#) und geteilter Verantwortung gilt für den Datenschutz in AWS Firewall Manager. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter [Häufig gestellte Fragen zum Datenschutz](#). Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag [AWS -Modell der geteilten Verantwortung und in der DSGVO](#) im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-2](#).

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Firewall Manager oder anderen Geräten arbeiten und die Konsole, die API oder AWS SDKs AWS-Services verwenden. AWS CLI Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine

Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Firewall Manager Manager-Entitäten — wie Richtlinien — werden im Ruhezustand verschlüsselt, außer in bestimmten Regionen, in denen Verschlüsselung nicht verfügbar ist, darunter China (Peking) und China (Ningxia). Eindeutige Verschlüsselungsschlüssel werden für jede Region verwendet.

Identity and Access Management für AWS Firewall Manager

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service, den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Firewall Manager Manager-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service, das Sie ohne zusätzliche Kosten nutzen können.

Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [Wie AWS Firewall Manager funktioniert mit IAM](#)
- [Beispiele für identitätsbasierte Richtlinien für AWS Firewall Manager](#)
- [AWS verwaltete Richtlinien für AWS Firewall Manager](#)
- [Problembehandlung bei AWS Firewall Manager Identität und Zugriff](#)
- [Verwenden von serviceverknüpften Rollen für Firewall Manager](#)
- [Serviceübergreifende Confused-Deputy-Prävention](#)

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Firewall Manager ausführen.

Dienstbenutzer — Wenn Sie den Firewall Manager Manager-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Da Sie für Ihre Arbeit mehr Funktionen von Firewall Manager verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle

nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie in Firewall Manager nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unter [Problembehandlung bei AWS Shield Identität und Zugriff](#).

Service-Administrator — Wenn Sie in Ihrem Unternehmen für die Ressourcen von Firewall Manager verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Firewall Manager. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Firewall Manager Ihre Service-Benutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Firewall Manager verwenden kann, finden Sie unter [Wie AWS Shield funktioniert mit IAM](#).

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Firewall Manager zu verwalten. Beispiele für identitätsbasierte Richtlinien von Firewall Manager, die Sie in IAM verwenden können, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Shield](#)

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportale anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter [So melden Sie sich bei Ihrem an AWS-Konto](#) im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen

Methode, um Anfragen selbst zu [signieren](#), finden Sie im [IAM-Benutzerhandbuch unter AWS API-Anfragen](#) signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter [Multi-Faktor-Authentifizierung](#) im AWS IAM Identity Center - Benutzerhandbuch und [Verwenden der Multi-Faktor-Authentifizierung \(MFA\) in AWS](#) im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie ein AWS-Konto erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter [Was ist IAM Identity Center?](#) im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Eine [IAM-Gruppe](#) ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter [Erstellen eines IAM-Benutzers \(anstatt einer Rolle\)](#) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen [wechseln](#). Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter [Verwenden von IAM-Rollen](#) im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- **Verbundbenutzerzugriff:** Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter [Erstellen von Rollen für externe](#)

[Identitätsanbieter](#) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze](#) im AWS IAM Identity Center -Benutzerhandbuch.

- Temporäre IAM-Benutzerberechtigungen: Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien](#) im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
- Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).
- Servicerolle: Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem

Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Anwendungen, die auf Amazon EC2 ausgeführt werden — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter [Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden](#) im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter [Erstellen einer IAM-Rolle \(anstatt eines Benutzers\)](#) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter [Auswahl zwischen verwalteten und eingebundenen Richtlinien](#) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen zu ACLs finden Sie unter [Zugriffssteuerungsliste \(ACL\) – Übersicht](#) (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- **Berechtigungsgrenzen:** Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im IAM-Benutzerhandbuch.
- **Service Control Policies (SCPs)** — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten, die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organisationen und SCPs finden Sie unter [Funktionsweise von SCPs](#) im AWS Organizations -Benutzerhandbuch.
- **Sitzungsrichtlinien:** Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und

der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

Wie AWS Firewall Manager funktioniert mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Firewall Manager zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen mit Firewall Manager verwendet werden können.

IAM-Funktionen, die Sie mit verwenden können AWS Firewall Manager

IAM-Feature	Unterstützung für Firewall Manager
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (servicespezifisch)	Nein
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Teilweise

IAM-Feature	Unterstützung für Firewall Manager
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie Firewall Manager und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im [IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren](#).

Identitätsbasierte Richtlinien für Firewall Manager

Unterstützt Richtlinien auf Identitätsbasis.	Ja
--	----

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien von Firewall Manager finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Firewall Manager](#)

Beispiele für identitätsbasierte Richtlinien für Firewall Manager

Beispiele für identitätsbasierte Richtlinien von Firewall Manager finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Firewall Manager](#)

Ressourcenbasierte Richtlinien in Firewall Manager

Unterstützt ressourcenbasierte Richtlinien	Nein
--	------

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter [Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden](#) im IAM-Benutzerhandbuch.

Richtlinienaktionen für Firewall Manager

Unterstützt Richtlinienaktionen

Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der Firewall Manager Manager-Aktionen finden Sie unter [Aktionen definiert von AWS Firewall Manager](#) in der Service Authorization Reference.

Richtlinienaktionen in Firewall Manager verwenden vor der Aktion das folgende Präfix:

```
fms
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [  
  "fms:action1",  
  "fms:action2"  
]
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "fms:Describe*"
```

Beispiele für identitätsbasierte Richtlinien von Firewall Manager finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Firewall Manager](#)

Richtlinienressourcen für Firewall Manager

Unterstützt Richtlinienressourcen

Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein `Resource` oder ein `NotResource`-Element enthalten.

Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen [Amazon-Ressourcennamen \(ARN\)](#) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*" 
```

Eine Liste der Firewall Manager Manager-Ressourcentypen und ihrer ARNs finden Sie unter [Resources defined by AWS Firewall Manager](#) in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter [Von AWS Firewall Manager definierte Aktionen](#).

Beispiele für identitätsbasierte Richtlinien von Firewall Manager finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Firewall Manager](#)

Schlüssel für Richtlinienbedingungen für Firewall Manager

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Nein
---	------

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition block`) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die [Bedingungsoperatoren](#) verwenden, z. B. `ist gleich` oder `kleiner als`, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet die Bedingung mithilfe einer logischen OR Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter [IAM-Richtlinienelemente: Variablen und Tags](#) im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [Kontextschlüssel für AWS globale Bedingungen](#) im IAM-Benutzerhandbuch.

Eine Liste der Bedingungsschlüssel von Firewall Manager finden Sie unter [Bedingungsschlüssel für AWS Firewall Manager](#) in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter [Aktionen definiert von AWS Firewall Manager](#).

Beispiele für identitätsbasierte Richtlinien von Firewall Manager finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Firewall Manager](#)

ACLs im Firewall Manager

Unterstützt ACLs	Nein
------------------	------

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit Firewall Manager

Unterstützt ABAC (Tags in Richtlinien)	Ja
--	----

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement einer [Richtlinie Tag-Informationen](#) an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter [Was ist ABAC?](#) im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe [Attributbasierte Zugriffskontrolle \(ABAC\)](#) verwenden im IAM-Benutzerhandbuch.

Temporäre Anmeldeinformationen mit Firewall Manager verwenden

Unterstützt temporäre Anmeldeinformationen	Ja
--	----

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services [funktionieren AWS-Services](#), finden Sie im [IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM](#).

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter [Wechseln zu einer Rolle \(Konsole\)](#) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter [Temporäre Sicherheitsanmeldeinformationen in IAM](#).

Zugriffssitzungen für Firewall Manager weiterleiten

Unterstützt Forward Access Sessions (FAS)	Ja
---	----

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

Servicerollen für Firewall Manager

Unterstützt Servicerollen

Teilweise

Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.

Warning

Durch das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von Firewall Manager beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, wenn Firewall Manager Sie dazu anleitet.

Auswahl einer IAM-Rolle in Firewall Manager

Um die *PutNotificationChannel* API-Aktion in Firewall Manager verwenden zu können, müssen Sie eine Rolle auswählen, mit der Firewall Manager auf Amazon SNS zugreifen kann, sodass der Service Amazon SNS SNS-Nachrichten in Ihrem Namen veröffentlichen kann. Weitere Informationen finden Sie [PutNotificationChannel](#) in der AWS Firewall Manager API-Referenz.

Im Folgenden finden Sie ein Beispiel für eine Berechtigungseinstellung für ein SNS-Thema. Um diese Richtlinie mit Ihrer eigenen benutzerdefinierten Rolle zu verwenden, ersetzen Sie den `AWSServiceRoleForFMS` Amazon-Ressourcennamen (ARN) durch den `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"
}
```

Weitere Informationen zu den Aktionen und Ressourcen von Firewall Manager finden Sie im AWS Identity and Access Management Leitfadenthema [Aktionen definiert von AWS Firewall Manager](#)

Serviceverknüpfte Rollen für Firewall Manager

Unterstützt serviceverknüpfte Rollen	Ja
--------------------------------------	----

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter [AWS -Services, die mit IAM funktionieren](#). Suchen Sie in der Tabelle nach einem Service mit einem Yes in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für AWS Firewall Manager

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Firewall Manager Manager-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Einzelheiten zu den von Firewall Manager definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Firewall Manager](#) in der Service Authorization Reference.

Themen

- [Bewährte Methoden für Richtlinien](#)
- [Verwenden der Firewall Manager Manager-Konsole](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)
- [Gewähren Sie Ihren Firewall Manager Manager-Sicherheitsgruppen Lesezugriff](#)
- [Vollzugriff auf AWS Firewall Manager Ressourcen gewähren](#)

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Firewall Manager Manager-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter [AWS -verwaltete Richtlinien](#) oder [AWS -verwaltete Richtlinien für Auftrags-Funktionen](#) im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten: Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter [Richtlinien und Berechtigungen in IAM](#) im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs: Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben,

um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: Bedingung](#) im IAM-Benutzerhandbuch.

- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten: IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter [Richtlinienvvalidierung zum IAM Access Analyzer](#) im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter [Konfigurieren eines MFA-geschützten API-Zugriffs](#) im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Bewährte Methoden für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

Verwenden der Firewall Manager Manager-Konsole

Um auf die AWS Firewall Manager Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Firewall Manager Manager-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die Firewall Manager-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch den Firewall Manager *ConsoleAccess* oder die *ReadOnly* AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter [Hinzufügen von Berechtigungen zu einem Benutzer](#) im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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": "*"
    }
  ]
}
```

Gewähren Sie Ihren Firewall Manager Manager-Sicherheitsgruppen Lesezugriff

Der Firewall Manager ermöglicht den kontoübergreifenden Zugriff auf Ressourcen, aber es ist nicht möglich, kontenübergreifenden Ressourcenschutz zu erstellen. Sie können Schutz für Ressourcen nur aus dem Konto erstellen, das der Besitzer dieser Ressourcen ist.

Im Folgenden finden Sie ein Beispiel für eine Richtlinie, die Berechtigungen für die `ec2:DescribeSecurityGroups` Aktionen `fms:Get*` und `fms:List*`, und für alle Ressourcen gewährt.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "fms:Get*",
        "fms:List*",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Vollzugriff auf AWS Firewall Manager Ressourcen gewähren

Folgen Sie dieser Anleitung, wenn Sie Schwierigkeiten haben, Ihre Firewall Manager-Richtlinien mit der verwalteten Richtlinie zu erstellen oder zu verwalten `AWSFMAAdminFullAccess`. Informationen zum Arbeiten mit verwalteten Richtlinien für AWS Firewall Manager finden Sie unter [Verwalten von Richtlinien für AWS Firewall Manager](#).

Diese Richtlinie beinhaltet keine Berechtigungen zum Einrichten von Amazon Simple Notification Service-Benachrichtigungen in AWS Firewall Manager. Informationen zum Einrichten des Zugriffs für Amazon Simple Notification Service finden Sie unter [Zugriff für Amazon Simple Notification Service einrichten](#).

Verwenden Sie die folgende Richtlinie, um vollen Administratorzugriff auf Ihr Konto zu gewähren:

```
{
  "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"
                ]
            }
        }
    }
]
}

```

Einzelheiten zur Genehmigung

Diese Richtlinie umfasst die folgenden Berechtigungen. :

- `fms:*`:

Ermöglicht es Ihnen, mit AWS Firewall Manager Ressourcen zu arbeiten.

- `waf:*`, `waf-regional:*`:

Ermöglicht das Arbeiten mit AWS WAF Richtlinien.

- `waf:*`, `waf-regional:*`:

Ermöglicht das Arbeiten mit AWS WAF Richtlinien.

- `elasticloadbalancing:SetWebACL`:

Ermöglicht das Zuordnen von Web Access Control Lists (ACLs) zu Elastic Load Balancers.

- `firehose:ListDeliveryStreams:`

Ermöglicht das Anzeigen AWS WAF von Protokollen.

- `organizations:DescribeAccount`, `organizations:DescribeOrganization`,
`organizations:ListRoots`, `organizations:ListChildren`,
`organizations:ListAccounts`, `organizations:ListAccountsForParent`,
`organizations:ListOrganizationalUnitsForParent:`

Ermöglicht die Zusammenarbeit mit AWS Organizations.

- `shield:GetSubscriptionState:`

Ermöglicht es Ihnen, den Abonnementstatus für eine AWS Shield Richtlinie anzuzeigen.

- `route53resolver:ListFirewallRuleGroups`,
`route53resolver:GetFirewallRuleGroup:`

Ermöglicht die Arbeit mit Regelgruppen von Route 53 Private DNS für VPCs in einer Richtlinie für Route 53 Private DNS für VPCs.

- `wafv2:ListRuleGroups`, `wafv2:ListAvailableManagedRuleGroups`,
`wafv2:CheckCapacity`, `wafv2:PutLoggingConfiguration`,
`wafv2:ListAvailableManagedRuleGroupVersions:`

Ermöglicht das Arbeiten mit AWS WAFV2 Richtlinien.

- `network-firewall:DescribeRuleGroup`, `network-`
`firewall:DescribeRuleGroupMetadata`, `network-firewall:ListRuleGroups:`

Ermöglicht das Arbeiten mit AWS Network Firewall Richtlinien.

- `ec2:DescribeAvailabilityZones:`

Ermöglicht das Anzeigen der Availability Zones einer AWS Network Firewall Richtlinie.

- `ec2:DescribeRegions:`

Ermöglicht es Ihnen, die Region einer Richtlinie in der AWS Firewall Manager Konsole anzuzeigen.

AWS verwaltete Richtlinien für AWS Firewall Manager

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie [kundenverwaltete Richtlinien](#) definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter [Von AWS verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSFMAAdminFullAccess

Verwenden Sie die `AWSFMAAdminFullAccess` AWS verwaltete Richtlinie, um Ihren Administratoren den Zugriff auf AWS Firewall Manager Ressourcen zu ermöglichen, einschließlich aller Firewall Manager Manager-Richtlinientypen. Diese Richtlinie beinhaltet keine Berechtigungen zum Einrichten von Amazon Simple Notification Service-Benachrichtigungen in AWS Firewall Manager. Informationen zum Einrichten des Zugriffs für Amazon Simple Notification Service finden Sie unter [Zugriff für Amazon Simple Notification Service einrichten](#).

Einzelheiten zur Genehmigung

Diese Richtlinie ist je nach Berechtigungssatz in Aussagen gruppiert.

- AWS Firewall Manager Richtlinienressourcen — Ermöglicht vollständige Administratorrechte für Ressourcen AWS Firewall Manager, einschließlich aller Firewall Manager Manager-Richtlinientypen.
- AWS WAF Protokolle in Amazon Simple Storage Service schreiben — Ermöglicht Firewall Manager das Schreiben und Lesen von AWS WAF Protokollen in Amazon S3.

- **Dienstverknüpfte Rolle erstellen** — Ermöglicht es dem Administrator, eine dienstverknüpfte Rolle zu erstellen, die es Firewall Manager ermöglicht, in Ihrem Namen auf Ressourcen in anderen Diensten zuzugreifen. Diese Berechtigung ermöglicht das Erstellen der dienstbezogenen Rolle nur für die Verwendung durch Firewall Manager. Informationen darüber, wie Firewall Manager dienstverknüpfte Rollen verwendet, finden Sie unter [Verwenden von serviceverknüpften Rollen für Firewall Manager](#).
- **AWS Organizations**— Ermöglicht Administratoren die Verwendung von Firewall Manager für eine Organisation in AWS Organizations. Nachdem der vertrauenswürdige Zugriff für Firewall Manager aktiviert wurde AWS Organizations, können Mitglieder des Administratorkontos die Ergebnisse in ihrer gesamten Organisation einsehen. Informationen zur Verwendung AWS Organizations mit AWS Firewall Manager finden Sie [unter Verwendung AWS Organizations mit anderen AWS Diensten](#) im AWS Organizations Benutzerhandbuch.

```
{
  "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"
            ]
        }
    }
}

```

```

    }
  }
]
}

```

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `fms:*`:

Ermöglicht das Arbeiten mit AWS Firewall Manager Ressourcen.

- `waf:*`, `waf-regional:*`:

Ermöglicht es Ihnen, mit AWS WAF Richtlinien zu arbeiten.

- `elasticloadbalancing:SetWebACL`:

Ermöglicht das Zuordnen von Web Access Control Lists (ACLs) zu Elastic Load Balancers.

- `firehose:ListDeliveryStreams`:

Ermöglicht das Anzeigen AWS WAF von Protokollen.

- `organizations:DescribeAccount`, `organizations:DescribeOrganization`,
`organizations:ListRoots`, `organizations:ListChildren`,
`organizations:ListAccounts`, `organizations:ListAccountsForParent`,
`organizations:ListOrganizationalUnitsForParent`:

Ermöglicht die Zusammenarbeit mit AWS Organizations.

- `shield:GetSubscriptionState`:

Ermöglicht es Ihnen, den Abonnementstatus für eine AWS Shield Richtlinie anzuzeigen.

- `route53resolver:ListFirewallRuleGroups`,
`route53resolver:GetFirewallRuleGroup`:

Ermöglicht die Arbeit mit Regelgruppen von Route 53 Private DNS für VPCs in einer Richtlinie für Route 53 Private DNS für VPCs.

- `wafv2:ListRuleGroups`, `wafv2:ListAvailableManagedRuleGroups`,
`wafv2:CheckCapacity`, `wafv2:PutLoggingConfiguration`,
`wafv2:ListAvailableManagedRuleGroupVersions`:

Ermöglicht das Arbeiten mit AWS WAFV2 Richtlinien.

- `network-firewall:DescribeRuleGroup`, `network-firewall:DescribeRuleGroupMetadata`, `network-firewall>ListRuleGroups`:
Ermöglicht das Arbeiten mit AWS Network Firewall Richtlinien.
- `ec2:DescribeAvailabilityZones`:
Ermöglicht das Anzeigen der Availability Zones einer AWS Network Firewall Richtlinie.
- `ec2:DescribeRegions`:
Ermöglicht es Ihnen, die Region einer Richtlinie in der AWS Firewall Manager Konsole anzuzeigen.
- `s3:GetBucketPolicy`:
Ermöglicht das Abrufen der Amazon S3 S3-Bucket-Richtlinie für AWS WAF Protokolle.
- `ListDelegatedAdministrators`:
Ermöglicht es Ihnen, delegierte Administratoren von Amazon OpenSearch Service aufzulisten.

AWS verwaltete Richtlinie: FMS ServiceRolePolicy

Diese Richtlinie ermöglicht AWS Firewall Manager die Verwaltung von AWS Ressourcen in Ihrem Namen im Firewall Manager und in integrierten Diensten. Diese Richtlinie ist mit der `AWSServiceRoleForFMS` dienstverknüpften Rolle verbunden. Weitere Informationen zur serviceverknüpften Rolle finden Sie unter [Verwenden von serviceverknüpften Rollen für Firewall Manager](#).

Einzelheiten zu den Richtlinien finden Sie in der IAM-Konsole bei [ServiceRolePolicyFMS](#).

AWS verwaltete Richtlinie: AWSFMAdminReadOnlyAccess

Gewährt schreibgeschützten Zugriff auf alle AWS Firewall Manager Manager-Ressourcen.

```
{
  "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"
      ]
    }
  }
}

```

```

    ]
  }
}
]
}
}
]
}
}
}

```

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `fms:*`:

Ermöglicht das Anzeigen AWS Firewall Manager von Ressourcen.

- `waf:Get*`, `waf-regional:Get*`:

Ermöglicht das Abrufen von AWS WAF Richtlinien.

- `waf:List*`, `waf-regional:List*`:

Ermöglicht das Auflisten von AWS WAF Richtlinien.

- `firehose:ListDeliveryStreams`:

Ermöglicht das Auflisten von AWS WAF Protokollen.

- `organizations:DescribeOrganization`, `organizations:DescribeAccount`,
`organizations:DescribeOrganization`, `organizations:ListRoots`,
`organizations:ListChildren`, `organizations:ListAccounts`,
`organizations:ListAccountsForParent`,
`organizations:ListOrganizationalUnitsForParent`:

Ermöglicht es Ihnen, die Ressourcen von AWS Organizations anzuzeigen.

- `shield:GetSubscriptionState`:

Ermöglicht das Abrufen des Abonnementstatus für eine AWS Shield Richtlinie.

- `route53resolver:ListFirewallRuleGroups`,
`route53resolver:GetFirewallRuleGroup`:

Ermöglicht das Abrufen und Auflisten von Regelgruppen für Route 53 Private DNS für VPCs in einer Route 53-Richtlinie für Private DNS für VPCs.

- `wafv2:ListRuleGroups`, `wafv2:ListAvailableManagedRuleGroups`,
`wafv2:CheckCapacity`, `wafv2:ListAvailableManagedRuleGroupVersions`:

Ermöglicht das Auflisten von AWS WAFV2 Regelgruppen, Regelgruppen für AWS verwaltete Regeln in AWS WAFV2 Richtlinien, AWS WAFV2 Regelgruppenkapazität und Versionen von Regelgruppen für AWS WAFV2 AWS verwaltete Regeln.

- `network-firewall:DescribeRuleGroup`, `network-firewall:DescribeRuleGroupMetadata`, `network-firewall>ListRuleGroups`:

Ermöglicht das Anzeigen von AWS Network Firewall Regelgruppen und Regelgruppen-Metadaten.

- `ec2:DescribeAvailabilityZones`:

Ermöglicht das Anzeigen der Availability Zones einer AWS Network Firewall Richtlinie.

- `ec2:DescribeRegions`:

Ermöglicht es Ihnen, die Region einer Richtlinie in der AWS Firewall Manager Konsole anzuzeigen.

- `s3:GetBucketPolicy`:

Ermöglicht das Abrufen der Amazon S3 S3-Bucket-Richtlinie für AWS WAF Protokolle.

- `ListDelegatedAdministrators`:

Ermöglicht es Ihnen, delegierte Administratoren in AWS Organizations aufzulisten.

AWS verwaltete Richtlinie: `AWSFMMemberReadOnlyAccess`

Gewährt nur Lesezugriff auf AWS Firewall Manager Mitgliederressourcen. Einzelheiten zu den Richtlinien finden Sie in der IAM-Konsole unter [AWSFMMemberReadOnlyAccess](#)

Firewall Manager Manager-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Firewall Manager an, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Wenn Sie automatische Benachrichtigungen über Änderungen an dieser Seite erhalten möchten, abonnieren Sie den RSS-Feed auf der Seite mit dem Dokumentverlauf von Firewall Manager unter [Dokumentverlauf](#).

Änderung	Beschreibung	Datum
FMS ServiceRolePolicy — Aktualisierte Richtlinie	<p>Es wurden Berechtigungen hinzugefügt, mit denen Firewall Manager beschreiben kann, ob die angegebenen AWS Config Regeln konform sind.</p> <p>Die aktualisierte Richtlinie finden Sie in der IAM-Konsole: ServiceRolePolicyFMS.</p>	21. April 2023
FMS ServiceRolePolicy — Aktualisierte Richtlinie	<p>Es wurden Berechtigungen hinzugefügt, die es Firewall Manager ermöglichen, Amazon EC2 EC2-Instance- und Netzwerkschnittstellenattribute zu beschreiben.</p> <p>Die aktualisierte Richtlinie finden Sie in der IAM-Konsole: FMS. ServiceRolePolicy</p>	15. November 2022
AWSFMAdminReadOnlyAccess — Aktualisierte Richtlinie	<p>Es wurden Berechtigungen zur Unterstützung von Shield AWS WAFV2, Network Firewall, DNS-Firewall, Amazon VPC-Sicherheitsgruppe und Richtlinien hinzugefügt.</p> <p>Die aktualisierte Richtlinie finden Sie in der IAM-Konsole: AWSFMAdminReadOnlyAccess</p>	02. November 2022

Änderung	Beschreibung	Datum
<p>AWSFMAdminFullAccess— Aktualisierte Richtlinie</p>	<p>Es wurden Berechtigungen zur Unterstützung von Shield AWS WAFV2, Network Firewall, DNS-Firewall, Amazon VPC-Sicherheitsgruppe und Richtlinien hinzugefügt. Amazon SNS SNS-Berechtigungen wurden entfernt.</p> <p>Die aktualisierte Richtlinie finden Sie in der IAM-Konsole: AWSFMAdminFullAccess</p>	<p>21. Oktober 2022</p>
<p>FMSServiceRolePolicy — Neue Berechtigungen für AWS Firewall Manager Firewall-Richtlinien von Drittanbietern</p>	<p>Diese Änderung ermöglicht es Firewall Manager, die Amazon EC2 EC2-VPC-Endpunkte zu erstellen und zu löschen, die mit einer Firewall-Richtlinie eines Drittanbieters verknüpft sind.</p>	<p>30. März 2022</p>
<p>FMSServiceRolePolicy — Neue Berechtigungen für Richtlinien AWS Network Firewall</p>	<p>Es wurden neue Berechtigungen hinzugefügt, um die Bereitstellung von Firewalls für Netzwerk-Firewall-Richtlinien zu unterstützen. Die neuen Berechtigungen ermöglichen das Abrufen von Informationen über Availability Zones für Konten, die in den Geltungsbereich einer Richtlinie fallen.</p>	<p>16. Februar 2022</p>

Änderung	Beschreibung	Datum
FMSServiceRolePolicy — Neue Berechtigungen für Richtlinien AWS Shield	Neue Berechtigungen zum Abrufen von Tags für AWS WAF regionale und AWS WAF globale Ressourcen hinzugefügt. Es wurden AWS WAF regionale Berechtigungen zum Abrufen von Web-ACLs mithilfe eines Ressourcen-ARN hinzugefügt. Es wurden Berechtigungen zur Unterstützung der automatischen DDoS-Abwehr auf Anwendungsebene von Shield hinzugefügt.	07. Januar 2022
FMSServiceRolePolicy — Neue Berechtigungen für AWS Shield Richtlinien	Neue Berechtigung zum Abrufen von Tags für Elastic Load Balancing Balancing-Ressourcen hinzugefügt.	18. November 2021
FMSServiceRolePolicy — Neue Berechtigungen für Sicherheitsgruppen und AWS Network Firewall Richtlinien	Neue Berechtigungen wurden hinzugefügt, um die zentrale Protokollierung von AWS Network Firewall Richtlinien zu ermöglichen. Darüber hinaus wurden Amazon EC2 EC2-Berechtigungen mit Lesezugriff hinzugefügt, um Änderungen am Config-Service zu unterstützen, die sich darauf auswirken, wie Ressourcen nach AWS Firewall Manager Sicherheitsgruppenrichtlinien abgefragt werden.	29. September 2021

Änderung	Beschreibung	Datum
FMSServiceRolePolicy — ARN-Formate für AWS WAF Ressourcen	Das wurde aktualisiert FMSServiceRolePolicy , um die ARN-Formate für AWS WAF Ressourcen zu standardisieren. Die aktualisierten ARN-Formate sind <code>arn:aws:waf:*:*:*</code> und <code>arn:aws:waf-regional:*:*:*</code> .	12. August 2021
FMSServiceRolePolicy — Weitere Regionen in China	AWS Firewall Manager hat FMSServiceRolePolicy für die Regionen BJS und ZHY in China aktiviert.	12. August 2021
FMSServiceRolePolicy — Aktualisierung der bestehenden Richtlinie	<p>Es wurden neue Berechtigungen hinzugefügt, um die Amazon Route 53 Resolver DNS-Firewall verwalten AWS Firewall Manager zu können.</p> <p>Diese Änderung ermöglicht es Firewall Manager, Amazon Route 53 Resolver DNS-Firewallzuordnungen zu konfigurieren. Auf diese Weise können Sie den Firewall Manager verwenden, um DNS-Firewall-Schutz für Ihre VPCs in Ihrer gesamten Organisation bereitzustellen. AWS Organizations</p>	17. März 2021

Änderung	Beschreibung	Datum
Firewall Manager hat begonnen, Änderungen zu verfolgen	Firewall Manager begann, Änderungen für seine AWS verwalteten Richtlinien zu verfolgen.	02. März 2021

Problembehandlung bei AWS Firewall Manager Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Firewall Manager und IAM auftreten können.

Themen

- [Ich bin nicht berechtigt, eine Aktion in Firewall Manager durchzuführen](#)
- [Ich bin nicht berechtigt, iam auszuführen: PassRole](#)
- [Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Firewall Manager Manager-Ressourcen ermöglichen](#)

Ich bin nicht berechtigt, eine Aktion in Firewall Manager durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven `my-example-widget`-Ressource anzuzeigen, jedoch nicht über `fms:GetWidget`-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
fms:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `fms:GetWidget`-Aktion auf die `my-example-widget`-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht autorisiert sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Firewall Manager übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Firewall Manager auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Firewall Manager Manager-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffssteuerungslisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Firewall Manager diese Funktionen unterstützt, finden Sie unter [Wie AWS Shield funktioniert mit IAM](#).
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter [Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen](#).

- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter [Gewähren von Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien](#) im IAM-Benutzerhandbuch.

Verwenden von serviceverknüpften Rollen für Firewall Manager

AWS Firewall Manager verwendet AWS Identity and Access Management (IAM) [dienstgebundene](#) Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Firewall Manager verknüpft ist. Dienstbezogene Rollen sind von Firewall Manager vordefiniert und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle erleichtert die Einrichtung von Firewall Manager, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Firewall Manager definiert die Berechtigungen seiner dienstbezogenen Rollen, und sofern nicht anders definiert, kann nur Firewall Manager seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann an keine andere IAM-Entität angefügt werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem die zugehörigen Ressourcen gelöscht wurden. Dadurch werden Ihre Firewall Manager Manager-Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceverknüpften Rollen unterstützen, finden Sie unter [AWS -Services, die mit IAM funktionieren](#). Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Dienstbezogene Rollenberechtigungen für Firewall Manager

AWS Firewall Manager verwendet den Namen der dienstverknüpften Rolle `AWSServiceRoleForFMS`, damit Firewall Manager in Ihrem Namen AWS Dienste zur Verwaltung von Firewall-Richtlinien und AWS Organizations Kontoressourcen aufrufen kann. Diese Richtlinie

ist der AWS verwalteten Rolle `AWSServiceRoleForFMS` zugeordnet. Weitere Informationen zur verwalteten Rolle finden Sie unter [AWS verwaltete Richtlinie: FMS ServiceRolePolicy](#).

Die mit dem `AWSServiceRoleForFMS` Dienst verknüpfte Rolle vertraut darauf, dass der Dienst Folgendes übernimmt die Rolle. `fms.amazonaws.com`

Die Rollenberechtigungsrichtlinie ermöglicht es Firewall Manager, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- `waf`- Verwalten Sie AWS WAF klassische Web-ACLs, Regelgruppenberechtigungen und die Web-ACLs-Verknüpfungen in Ihrem Konto.
- `ec2`- Verwalten Sie Sicherheitsgruppen auf elastischen Netzwerkschnittstellen und Amazon EC2 EC2-Instances.
- `vpc`- Verwalten Sie Subnetze, Routing-Tabellen, Tags und Endpunkte in Amazon VPC.
- `wafv2`- Verwalten Sie AWS WAF Web-ACLs, Regelgruppenberechtigungen und die Web-ACLs-Verknüpfungen in Ihrem Konto.
- `cloudfront`- Erstellen Sie Web-ACLs, um Distributionen zu schützen. CloudFront
- `config`- Verwalte AWS Config Regeln, die dem Firewall Manager gehören, in deinem Konto.
- `iam`- Verwaltet diese dienstbezogene Rolle und erstellt erforderliche AWS WAF Rollen und dienstgebundene Shield-Rollen, wenn Sie die Protokollierung für AWS WAF und Shield-Richtlinien konfigurieren.
- `organization`- Erstellen Sie eine dienstbezogene Rolle, die Firewall Manager gehört, um die von Firewall Manager verwendeten AWS Organizations Ressourcen zu verwalten.
- `shield`- Verwalten Sie AWS Shield Schutzmaßnahmen und Konfigurationen zur L7-Abwehr für Ressourcen in Ihrem Konto.
- `ram`- Verwalten Sie die gemeinsame Nutzung von AWS RAM Ressourcen für DNS-Firewall-Regelgruppen und Netzwerk-Firewall-Regelgruppen.
- `network-firewall`- Verwalten Sie Firewall Manager-eigene AWS Network Firewall Ressourcen und abhängige Amazon VPC-Ressourcen in Ihrem Konto.
- `route53resolver`- Verwalten Sie DNS-Firewall-Verknüpfungen, die dem Firewall Manager gehören, in Ihrem Konto.

[Die vollständige Richtlinie finden Sie in der IAM-Konsole: FMS. ServiceRolePolicy](#)

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [serviceverknüpfte Rollenberechtigungen](#) im IAM-Benutzerhandbuch.

Eine serviceverknüpfte Rolle für Firewall Manager erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie die AWS Management Console Firewall Manager-Anmeldung am aktivieren oder eine `PutLoggingConfiguration` Anfrage in der Firewall Manager Manager-CLI oder der Firewall Manager Manager-API stellen, erstellt Firewall Manager die dienstbezogene Rolle für Sie.

Sie müssen über die `iam:CreateServiceLinkedRole`-Berechtigung verfügen, um die Protokollierung zu aktivieren.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie die Firewall Manager-Protokollierung aktivieren, erstellt Firewall Manager die dienstbezogene Rolle erneut für Sie.

Bearbeiten einer serviceverknüpften Rolle für Firewall Manager

Mit Firewall Manager können Sie die `AWSServiceRoleForFMS` dienstverknüpfte Rolle nicht bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Firewall Manager

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpften Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Note

Wenn der Firewall Manager Manager-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um die mit dem Dienst verknüpfte Rolle mithilfe von IAM zu löschen

Verwenden Sie die IAM-Konsole, die IAM-CLI oder die IAM-API, um die serviceverknüpfte Rolle zu löschen. `AWSServiceRoleForFMS` Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Leitfaden.

Unterstützte Regionen für serviceverknüpfte Firewall Manager Manager-Rollen

Firewall Manager unterstützt die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen der Dienst verfügbar ist. Weitere Informationen finden Sie unter [Firewall Manager Manager-Endpunkte und Kontingente](#).

Serviceübergreifende Confused-Deputy-Prävention

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiertere Entität zur Durchführung der Aktion zwingen kann. In AWS kann ein dienstübergreifendes Identitätswechsels zu einem Problem mit dem verwirrten Stellvertreter führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der aufrufende Service kann manipuliert werden, um seine Berechtigungen zu verwenden, um Aktionen auf die Ressourcen eines anderen Kunden auszuführen, für die er sonst keine Zugriffsberechtigung haben sollte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen, die Kontextschlüssel [aws:SourceArn](#) und die [aws:SourceAccount](#) globalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die der AWS Firewall Manager Ressource einen anderen Dienst gewähren. Verwenden Sie `aws:SourceArn`, wenn Sie nur eine Ressource mit dem betriebsübergreifenden Zugriff verknüpfen möchten. Verwenden Sie `aws:SourceAccount`, wenn Sie zulassen möchten, dass Ressourcen in diesem Konto mit der betriebsübergreifenden Verwendung verknüpft werden.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den globalen Kontextbedingungsschlüssel `aws:SourceArn` mit Platzhalterzeichen (*) für die unbekanntenen Teile des ARN. z. B. `arn:aws:fms:*:account-id:*`.

Wenn der `aws:SourceArn`-Wert die Konto-ID nicht enthält, z. B. einen Amazon-S3-Bucket-ARN, müssen Sie beide globale Bedingungskontextschlüssel verwenden, um Berechtigungen einzuschränken.

Der Wert von `aws:SourceArn` muss das AWS Firewall Manager AWS Administratorkonto sein.

Die folgenden Beispiele zeigen, wie Sie den `aws:SourceArn` globalen Bedingungskontextschlüssel in Firewall Manager verwenden können, um das Problem des verwirrten Stellvertreters zu verhindern.

Das folgende Beispiel zeigt, wie Sie das Problem mit dem verwirrten Stellvertreter verhindern können, indem Sie den `aws:SourceArn` globalen Bedingungskontextschlüssel in der Firewall Manager Rollenvertrauensrichtlinie verwenden. Ersetzen Sie *Region* und *Konto-ID* durch Ihre eigenen Informationen.

```
{
  "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"
      }
    }
  }
}
```

Protokollierung und Überwachung in Firewall Manager

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Firewall Manager und Ihren AWS Lösungen. Sie sollten Überwachungsdaten aus allen Teilen Ihrer AWS Lösung sammeln, damit Sie einen etwaigen Ausfall an mehreren Stellen leichter debuggen können. AWS bietet verschiedene Tools zur Überwachung Ihrer Firewall Manager Manager-Ressourcen und zur Reaktion auf potenzielle Ereignisse:

CloudWatch Amazon-Alarme

Mithilfe von CloudWatch Alarmen beobachten Sie eine einzelne Metrik über einen von Ihnen festgelegten Zeitraum. Wenn die Metrik einen bestimmten Schwellenwert überschreitet, CloudWatch sendet eine Benachrichtigung an ein Amazon SNS SNS-Thema oder eine AWS Auto Scaling Richtlinie. Weitere Informationen finden Sie unter [Überwachung mit Amazon CloudWatch](#).

AWS CloudTrail Logs

CloudTrail bietet eine Aufzeichnung der Aktionen, die von einem Benutzer, einer Rolle oder einem AWS Dienst in Firewall Manager ausgeführt wurden. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Firewall Manager gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln. Weitere Informationen finden Sie unter [Protokollierung von AWS CloudTrail-API-Aufrufen mit](#).

Konformitätsprüfung für Firewall Manager

Informationen darüber, ob AWS-Service ein [AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter](#) . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter [AWS Compliance-Programme AWS](#) .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter [Berichte herunterladen unter](#) .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- [Schnellstartanleitungen zu Sicherheit und Compliance](#) — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

Note

AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der [Referenz für HIPAA-berechtigte Services](#).

- [AWS Compliance-Ressourcen](#) — Diese Sammlung von Arbeitsmapen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- [AWS Leitfäden zur Einhaltung von Vorschriften für Kunden](#) — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- [Evaluierung von Ressourcen anhand von Regeln](#) im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.

- [AWS Security Hub](#)— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der [Security-Hub-Steuerungsreferenz](#).
- [AWS Audit Manager](#)— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz im Firewall Manager

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter [AWS Globale](#) Infrastruktur.

Sicherheit der Infrastruktur in AWS Firewall Manager

Als verwalteter Dienst AWS Firewall Manager ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter [AWS Cloud-Sicherheit](#). Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Firewall Manager zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit [AWS Security Token Service](#) (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

AWS Firewall Manager Kontingente

AWS Firewall Manager unterliegt den folgenden Kontingenten (früher als Beschränkungen bezeichnet).

AWS Firewall Manager hat Standardkontingente, die Sie möglicherweise erhöhen können, und feste Kontingente.

Die von Firewall Manager verwalteten Sicherheitsgruppenrichtlinien unterliegen den standardmäßigen Amazon VPC-Kontingenten. Weitere Informationen finden Sie unter [Amazon VPC-Kontingente](#) im [Amazon VPC-Benutzerhandbuch](#).

Jede Firewall Manager Manager-Netzwerk-Firewall-Richtlinie erstellt eine Netzwerk-Firewall-Firewall mit einer zugehörigen Firewall-Richtlinie und ihren Regelgruppen. Diese Netzwerk-Firewall-Ressourcen unterliegen den Kontingenten, die im Network Firewall Developer Guide unter [AWS Network Firewall Kontingente](#) aufgeführt sind.

Weiche Kontingente

AWS Firewall Manager hat Standardkontingente für die Anzahl der Entitäten pro Region. Sie können [eine Erhöhung dieser Kontingente beantragen](#).

Alle Richtlinientypen

Ressource	Standardkontingent pro Region
Konten pro Organisation in AWS Organizations	Variiert. Eine an ein Konto gesendete Einladung wird auf dieses Kontingent angerechnet. Die Anrechnung entfällt, wenn das eingelade

Ressource	Standardkontingent pro Region
	ne Konto ablehnt, das Verwaltungskonto die Einladung ablehnt oder die Einladung abgelaufen ist.
Firewall Manager Manager-Richtlinien pro Organisation in AWS Organizations.	50. Die Regionsangaben Global und US East (N. Virginia) Region beziehen sich auf dieselbe Region, sodass dieser Grenzwert für die Summe der kombinierten Richtlinien für beide gilt.
Organisationseinheiten im Geltungsbereich gemäß Firewall Manager Manager-Richtlinie.	20
Konten im Geltungsbereich einer Firewall Manager Manager-Richtlinie, wenn Sie einzelne Konten explizit ein- und ausschließen.	200
Konten im Geltungsbereich einer Firewall Manager Manager-Richtlinie, wenn Sie einzelne Konten nicht explizit ein- oder ausschließen.	2.500
Tags, die Ressourcen pro Firewall Manager Manager-Richtlinie einschließen oder ausschließen.	8
Maximale Anzahl von Ressourcensätzen pro Konto.	20
Maximale Anzahl von Ressourcen pro Ressourcensatz.	100
Maximale Anzahl von Ressourcensätzen pro Firewall Manager Manager-Richtlinie.	5

Gemeinsame Sicherheitsgruppenrichtlinien

Ressource	Standardkontingent pro Region.
Primäre Sicherheitsgruppen pro Richtlinie.	3
Amazon VPC-Instances im Umfang pro Richtlinie pro Konto, einschließlich gemeinsam genutzter VPCs.	100

Inhaltsprüfungssicherheitsgruppenrichtlinien

Ressource	Standardkontingent pro Region
Sicherheitsgruppen pro Richtlinie prüfen.	1
Liste der Anwendungen pro Anwendung.	50
Benutzerdefinierte verwaltete Anwendungslisten für Regeln, die den gesamten Datenverkehr zulassen.	1
Benutzerdefiniert verwaltete Anwendungslisten nach Richtlinienregeln.	1
Benutzerdefinierte verwaltete Anwendungslisten pro Konto.	10
Liste der Protokolle pro Protokoll.	5
Benutzerdefinierte verwaltete Protokolllisten für jede Einstellung in einer Richtlinie.	1
Listen mit benutzerdefinierten verwalteten Protokollen pro Konto.	10

AWS WAF Richtlinien

Ressource	Standardkontingent pro Region
AWS WAF Regelgruppen pro Firewall Manager Manager-Administratorkonto.	100
AWS WAF Klassische Regelgruppen pro Firewall Manager Manager-Administratorkonto.	10
Regelgruppen pro AWS WAF Richtlinie.	50

DNS-Firewall-Richtlinien

Ressource	Standardkontingent pro Region
DNS-Firewall-Regelgruppen pro Firewall Manager Manager-Richtlinie.	2

Feste Kontingente

Die folgenden regionalen Kontingente, die sich auf Folgendes beziehen, AWS Firewall Manager können nicht geändert werden.

Alle Richtlinientypen

Ressource	Kontingent pro Region
Die maximale Anzahl von Firewall Manager Manager-Administratoren, die Sie in einer AWS Organizations Organisation haben können. Sie müssen über einen Standardadministrator und bis zu neun weitere Firewall Manager Manager-Administratoren verfügen.	10

Netzwerk-Firewall-Richtlinien

Ressource	Kontingent pro Region
Anzahl der VPCs, die für eine einzelne Richtlinie automatisch repariert werden können.	1.000
Die Anzahl der IPV4-CIDRs, die Sie für eine einzelne Richtlinie bereitstellen können.	50

Richtlinien für die Inhaltsüberwachung von Sicherheitsgruppen

Ressource	Kontingent pro Region
Firewall Manager verwaltete Anwendungslisten für jede Einstellung in einer Richtlinie.	1
Von Firewall Manager verwaltete Protokolllisten für jede Einstellung in einer Richtlinie.	1

AWS WAF Richtlinien

Ressource	Kontingent pro Region
Gesamtzahl der Web ACL Capacity Units (WCU) für die Regelgruppen in einer AWS WAF -Richtlinie.	5,000

AWS WAF Klassische Richtlinien

Ressource	Kontingent pro Region
AWS WAF Klassische Regelgruppen pro Richtlinie.	2:1 vom Kunden erstellte Regelgruppe und 1 AWS Marketplace Regelgruppe.
AWS WAF Klassische Regeln pro Firewall Manager AWS WAF Classic-Regelgruppe.	10

Überwachung AWS WAFAWS Firewall Manager, und AWS Shield Advanced

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer Dienste.

Note

Informationen zur Überwachung Ihrer Shield Advanced-Ressourcen und zur Identifizierung möglicher DDoS-Ereignisse mithilfe von Shield Advanced finden Sie unter [AWS Shield](#).

Vor der Überwachung dieser Services sollten Sie einen Überwachungsplan erstellen, der Antworten auf die folgenden Fragen enthält:

- Was sind Ihre Ziele bei der Überwachung?
- Welche Ressourcen werden überwacht?
- Wie oft werden diese Ressourcen überwacht?
- Welche Überwachungstools werden verwendet?
- Wer soll die Überwachungsaufgaben ausführen?
- Wer soll benachrichtigt werden, wenn Fehler auftreten?

Im nächsten Schritt legen Sie einen Ausgangswert für normale Performance in Ihrer Umgebung fest, indem Sie die Leistung zu verschiedenen Zeiten und unter verschiedenen Lastbedingungen messen. Während der Überwachung AWS WAF speichern Firewall Manager, Shield Advanced und verwandte Dienste historische Überwachungsdaten, damit Sie sie mit aktuellen Leistungsdaten vergleichen, normale Leistungsmuster und Leistungsanomalien identifizieren und Methoden zur Behebung von Problemen entwickeln können.

Denn Sie sollten mindestens die folgenden Elemente überwachen AWS WAF, um eine Ausgangsbasis zu erstellen:

- Die Anzahl der zulässigen Webanforderungen
- Die Anzahl der blockierten Webanforderungen

Themen

- [Überwachungstools](#)
- [Überwachung mit Amazon CloudWatch](#)
- [Protokollierung von AWS CloudTrail-API-Aufrufen mit](#)

Überwachungstools

AWS bietet verschiedene Tools, mit denen Sie überwachen AWS WAF und AWS Shield Advanced. Sie können einige dieser Tools für die Überwachung konfigurieren, während andere manuellen Eingriff erfordern. Wir empfehlen, dass Sie die Überwachungsaufgaben möglichst automatisieren.

Automatisierte Überwachungstools


Sie können die folgenden automatisierten Überwachungstools verwenden, um zu beobachten AWS WAF AWS Shield Advanced und zu melden, wenn etwas nicht stimmt:

- Dashboards zur Übersicht über den Web-ACL-Traffic — Sie können auf Zusammenfassungen des Web-Traffics zugreifen, den eine Web-ACL auswertet. Rufen Sie dazu in der AWS WAF Konsole die Seite der Web-ACL auf und öffnen Sie dort die Registerkarte Traffic-Übersicht.

Die Traffic-Übersichts-Dashboards bieten fast in Echtzeit Zusammenfassungen der CloudWatch Amazon-Metriken, die bei der Auswertung des Web-Traffics Ihrer Anwendung AWS WAF erfasst werden. Sie können sich Zusammenfassungen für Ihren gesamten Web-Traffic und für den Traffic anzeigen lassen, der von den Regelgruppen zur intelligenten Bedrohungsabwehr ausgewertet wurde.

Weitere Informationen finden Sie unter [Dashboards zur Übersicht über den Web-ACL-Verkehr](#) oder in den Dashboards in der Konsole.

- Amazon CloudWatch Alarms — Überwachen Sie eine einzelne Metrik über einen von Ihnen angegebenen Zeitraum und führen Sie eine oder mehrere Aktionen aus, die auf dem Wert der Metrik im Verhältnis zu einem bestimmten Schwellenwert über mehrere Zeiträume basieren. Bei der Aktion handelt es sich um eine Benachrichtigung, die an ein Amazon Simple Notification Service (Amazon SNS)-Thema oder eine Amazon EC2 Auto Scaling-Richtlinie gesendet wird. Alarme rufen nur Aktionen für anhaltende Statusänderungen aus. CloudWatch Alarme lösen keine Aktionen aus, nur weil sie sich in einem bestimmten Zustand befinden. Der Status muss sich geändert haben und für eine bestimmte Anzahl von Zeiträumen beibehalten worden sein. Weitere Informationen finden Sie unter [CloudFrontAktivität überwachen mithilfe von CloudWatch](#).

 Note

CloudWatch Metriken und Alarme sind nicht aktiviert für AWS Firewall Manager.

Sie können die Advanced-Metriken nicht nur CloudWatch zur Überwachung AWS WAF und Shield verwenden [Überwachung mit Amazon CloudWatch](#), wie unter beschrieben, sondern Sie sollten sie auch CloudWatch zur Überwachung der Aktivitäten Ihrer geschützten Ressourcen verwenden. Weitere Informationen finden Sie hier:

- [CloudFront Aktivitäten überwachen — Verwenden CloudWatch](#) im Amazon CloudFront Developer Guide
- [Protokollierung und Überwachung in Amazon API Gateway](#) im API Gateway Developer Guide
- [CloudWatch Metriken für Ihren Application Load Balancer](#) im Elastic Load Balancing Balancing-Benutzerhandbuch
- [Überwachung und Protokollierung](#) im AWS AppSync Entwicklerhandbuch
- [Protokollierung und Überwachung in Amazon Cognito](#) im Amazon Cognito Developer Guide
- [Anzeige von App Runner-Protokollen, die in Logs gestreamt wurden, CloudWatch](#) und [Anzeige von App Runner-Servicemetriken, über die CloudWatch im Entwicklerhandbuch berichtet wurde](#) AWS App Runner
- Amazon CloudWatch Logs — Überwachen, speichern und greifen Sie auf Ihre Protokolldateien aus AWS CloudTrail oder anderen Quellen zu. Weitere Informationen finden Sie unter [Was ist Amazon CloudWatch Logs?](#) .
- Amazon CloudWatch Events — Automatisieren Sie Ihre AWS Services und reagieren Sie automatisch auf Systemereignisse. Ereignisse aus AWS Services werden nahezu in Echtzeit an CloudWatch Events übermittelt, und Sie können automatische Aktionen festlegen, die ergriffen werden, wenn ein Ereignis einer von Ihnen erstellten Regel entspricht. Weitere Informationen finden Sie unter [Was ist Amazon CloudWatch Events?](#)
- AWS CloudTrail Protokollüberwachung — Teilen Sie Protokolldateien zwischen Konten, überwachen CloudTrail Sie Protokolldateien in Echtzeit, indem Sie sie an CloudWatch Logs senden, schreiben Sie Anwendungen zur Protokollverarbeitung in Java und stellen Sie sicher, dass sich Ihre Protokolldateien nach der Lieferung von nicht geändert haben. CloudTrail Weitere Informationen finden Sie unter [Protokollierung von AWS CloudTrail-API-Aufrufen mit](#) und [Arbeiten mit CloudTrail Protokolldateien](#) im AWS CloudTrail Benutzerhandbuch.

- **AWS Config**— Sehen Sie sich die Konfiguration der AWS Ressourcen in Ihrem AWS Konto an, einschließlich der Beziehung zwischen den Ressourcen und ihrer Konfiguration in der Vergangenheit, sodass Sie sehen können, wie sich die Konfigurationen und Beziehungen im Laufe der Zeit ändern.

Manuelle Überwachungstools

Ein weiterer wichtiger Teil der Überwachung AWS WAF ist die AWS Shield Advanced manuelle Überwachung der Elemente, die von den CloudWatch Alarmen nicht abgedeckt werden. Sie können die Dashboards AWS WAF, Shield Advanced und andere AWS Management Console Dashboards aufrufen CloudWatch, um den Status Ihrer AWS Umgebung zu sehen. Wir empfehlen Ihnen, auch die Protokolldateien für Ihre Web-ACLs und Regeln zu überprüfen.

- Um beispielsweise das AWS WAF Dashboard anzuzeigen:
 - Sehen Sie sich auf der Seite AWS WAF Web-ACLs auf der Registerkarte Anfragen ein Diagramm mit der Gesamtzahl der Anfragen und der Anforderungen an, die jeder von Ihnen erstellten Regel entsprechen. Weitere Informationen finden Sie unter [Anzeigen einer Stichprobe von Webanforderungen](#).
- Sehen Sie sich die CloudWatch Startseite für Folgendes an:
 - Aktuelle Alarme und Status
 - Diagramme mit Alarmen und Ressourcen
 - Servicestatus

Darüber hinaus können CloudWatch Sie Folgendes verwenden:

- Erstellen Sie [benutzerdefinierte Dashboards](#) zur Überwachung der Services, die Ihnen wichtig sind.
- Aufzeichnen von Metrikdaten, um Probleme zu beheben und Trends zu erkennen.
- Suchen und durchsuchen Sie alle Ihre AWS Ressourcenmetriken.
- Erstellen und Bearbeiten von Alarmen, um über Probleme benachrichtigt zu werden.

Überwachung mit Amazon CloudWatch

Sie können Webanfragen, Web-ACLs und Regeln mithilfe von Amazon überwachen. Amazon CloudWatch sammelt und verarbeitet Rohdaten aus AWS WAF lesbaren, nahezu AWS Shield Advanced in Echtzeit verfügbaren Metriken. Sie können Statistiken in Amazon verwenden

CloudWatch , um sich einen Überblick über die Leistung Ihrer Webanwendung oder Ihres Dienstes zu verschaffen. Weitere Informationen finden Sie unter [Was steht CloudWatch](#) im CloudWatch Amazon-Benutzerhandbuch.

Note

CloudWatch Metriken und Alarme sind für Firewall Manager nicht aktiviert.

Sie können einen CloudWatch Amazon-Alarm erstellen, der eine Amazon SNS-Nachricht sendet, wenn sich der Status des Alarms ändert. Ein Alarm überwacht eine Metrik über einen bestimmten, von Ihnen definierten Zeitraum und führt eine oder mehrere Aktionen durch, die vom Wert der Metrik im Verhältnis zu einem bestimmten Schwellenwert in einer Reihe von Zeiträumen abhängt. Die Aktion ist eine Benachrichtigung, die an ein Amazon SNS-Thema oder eine Auto Scaling-Richtlinie gesendet wird. Alarme rufen nur Aktionen für anhaltende Statusänderungen hervor. CloudWatch Alarme lösen keine Aktionen aus, nur weil sie sich in einem bestimmten Zustand befinden. Der Zustand muss sich geändert haben und für eine bestimmte Anzahl von Zeiträumen beibehalten worden sein.

Themen

- [Anzeigen von -Metriken und -Dimensionen](#)
- [AWS WAF Metriken und Dimensionen](#)
- [AWS Shield Advanced Metriken](#)
- [AWS Firewall Manager Benachrichtigungen](#)

Anzeigen von -Metriken und -Dimensionen

Metriken werden zuerst nach dem Service-Namespace und dann nach den verschiedenen Dimensionskombinationen innerhalb der einzelnen Namespaces gruppiert. AWS Firewall Manager zeichnet keine Metriken auf.

- Der AWS WAF Namespace ist `AWS/WAFV2`
- Der Shield Advanced-Namespace ist `AWS/DDoSProtection`

Note

AWS WAF meldet Metriken einmal pro Minute.

Shield Advanced meldet Metriken einmal pro Minute während eines Ereignisses und seltener zu anderen Zeiten.

Gehen Sie wie folgt vor, um die Metriken für AWS WAF und anzuzeigen AWS Shield Advanced.

So zeigen Sie Metriken mit der CloudWatch Konsole an

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Ändern Sie bei Bedarf die Region in die Region, in der sich Ihre AWS Ressourcen befinden. Wählen Sie für CloudFront die Region USA Ost (Nord-Virginia) aus.
3. Wählen Sie im Navigationsbereich unter Metriken die Option Alle Metriken aus und suchen Sie dann auf der Registerkarte Durchsuchen nach dem Service.

So zeigen Sie Metriken mit der AWS CLI an

- Verwenden Sie für AWS/WAFV2 an einer Eingabeaufforderung den folgenden Befehl:

```
aws cloudwatch list-metrics --namespace "AWS/WAFV2"
```

Verwenden Sie für Shield Advanced an einer Eingabeaufforderung den folgenden Befehl:

```
aws cloudwatch list-metrics --namespace "AWS/DDoSProtection"
```

AWS WAF Metriken und Dimensionen

AWS WAF meldet Metriken einmal pro Minute. AWS WAF stellt Metriken und Dimensionen im AWS/WAFV2 Namespace bereit.

In der AWS WAF Konsole auf der Registerkarte „Traffic Overview“ der Web-ACL finden Sie zusammenfassende Informationen zu AWS WAF Metriken. Weitere Informationen finden Sie in der Konsole oder unter [Dashboards zur Übersicht über den Web-ACL-Verkehr](#).

Sie können die folgenden Metriken für Web-ACLs, Regeln, Regelgruppen und Labels einsehen.

- Ihre Regeln — Metriken sind nach der Regelaktion gruppiert. Wenn Sie beispielsweise eine Regel im Count Modus testen, werden ihre Treffer als Count Metriken für die Web-ACL aufgeführt.
- Ihre Regelgruppen — Die Metriken für Ihre Regelgruppen sind unter den Regelgruppen-Metriken aufgeführt.
- Regelgruppen, die einem anderen Konto gehören — Regelgruppen-Metriken sind in der Regel nur für den Eigentümer der Regelgruppe sichtbar. Wenn Sie jedoch die Regelaktion für eine Regel überschreiben, werden die Metriken für diese Regel unter Ihren Web-ACL-Metriken aufgeführt. Darüber hinaus werden Labels, die von einer beliebigen Regelgruppe hinzugefügt wurden, in Ihren Web-ACL-Metriken aufgeführt

Regelgruppen in dieser Kategorie sind [AWS Verwaltete Regeln für AWS WAF](#), [AWS Marketplace verwaltete Regelgruppen](#) [Regelgruppen, die von anderen Services bereitgestellt werden](#), und Regelgruppen, die von einem anderen Konto mit Ihnen geteilt wurden.

- Labels — Labels, die während der Evaluierung zu einer Webanfrage hinzugefügt wurden, werden in den Web-ACL-Label-Metriken aufgeführt. Sie können auf die Metriken für alle Labels zugreifen, unabhängig davon, ob sie durch Ihre Regeln und Regelgruppen oder durch Regeln in einer Regelgruppe hinzugefügt wurden, die einem anderen Konto gehört.

Themen

- [Metriken und Dimensionen für Web-ACL, Regelgruppen und Regeln](#)
- [Kennzeichnen Sie Metriken und Dimensionen](#)
- [Kostenlose Messwerte und Dimensionen zur Bot-Sichtbarkeit](#)

Metriken und Dimensionen für Web-ACL, Regelgruppen und Regeln

Web-ACL, Regelgruppe und Regelmetriken

Metrik	Beschreibung
AllowedRequests	Die Anzahl der zulässigen Webanforderungen. Berichtkriterien: Ein Wert ungleich Null. Gültige Statistiken: Summe
BlockedRequests	Die Anzahl der blockierten Webanforderungen.

Metrik	Beschreibung
	<p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Gültige Statistiken: Summe</p>
CountedRequests	<p>Die Anzahl der gezählten Webanforderungen.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Eine gezählte Webanforderung ist eine, die mindestens einer der Regeln entspricht. Anforderungszählung wird normalerweise zum Testen verwendet.</p> <p>Gültige Statistiken: Summe</p>
CaptchaRequests	<p>Die Anzahl der Webanfragen, auf die CAPTCHA-S teurelemente angewendet wurden.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Eine CAPTCHA-Webanforderung entspricht einer Regel mit einer Aktionseinstellung. CAPTCHA Diese Metrik zeichnet alle übereinstimmenden Anfragen auf, unabhängig davon, ob sie über ein gültiges CAPTCHA-Token verfügen.</p> <p>Gültige Statistiken: Summe</p>
RequestsWithValidCaptchaToken	<p>Die Anzahl der Webanfragen, auf die CAPTCHA-S teurelemente angewendet wurden und die über ein gültiges CAPTCHA-Token verfügten.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Gültige Statistiken: Summe</p>

Metrik	Beschreibung
CaptchasAttempted	<p>Die Anzahl der Lösungen, die von einem Endbenutzer als Antwort auf eine CAPTCHA-Puzzle-Herausforderung eingereicht wurden.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Gültige Statistiken: Summe</p>
CaptchasSolved	<p>Die Anzahl der eingereichten CAPTCHA-Rätselösungen, mit denen das Rätsel erfolgreich gelöst wurde.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Gültige Statistiken: Summe</p>
ChallengeRequests	<p>Die Anzahl der Webanfragen, für die Challenge-Kontrollen angewendet wurden.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Eine Challenge-Webanforderung entspricht einer Regel, die über eine Challenge Aktionseinstellung verfügt. Diese Metrik zeichnet alle übereinstimmenden Anfragen auf, unabhängig davon, ob sie über ein gültiges Challenge-Token verfügen.</p> <p>Gültige Statistiken: Summe</p>
RequestsWithValidChallengeToken	<p>Die Anzahl der Webanfragen, für die Challenge-Kontrollen angewendet wurden und für die ein gültiges Challenge-Token verwendet wurde.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Gültige Statistiken: Summe</p>

Metrik	Beschreibung
PassedRequests	<p>Die Anzahl der bestandenen Anfragen. Dies wird nur für Anfragen verwendet, die einer Regelgruppenbewertung unterzogen werden, ohne einer der Regelgruppenregeln zu entsprechen.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Bei übergebenen Anfragen handelt es sich um Anfragen, die keiner der Regeln in der Regelgruppe entsprechen.</p> <p>Gültige Statistiken: Summe</p>

Web-ACL, Regelgruppe und Regeldimensionen

Dimension	Beschreibung
Region	Erforderlich für alle geschützten Ressourcentypen außer für CloudFront Amazon-Distributionen.
Rule	<p>Eine der beiden folgenden Komponenten:</p> <ul style="list-style-type: none"> • Der Metrikname der Rule. • ALL steht für alle Regeln innerhalb einer WebACL oder RuleGroup . • Default_Action (nur in Kombination mit der WebACL Dimension), die die Aktion darstellt , die einer Anfrage zugewiesen wurde, deren Bewertung nicht durch die Aktion einer Regel in der Web-ACL beendet wurde.
RuleGroup	Der Metrikname der RuleGroup .
WebACL	Der Metrikname der WebACL.
Country	Das Ursprungsland der Anfrage. Dies ist die zweistellige Bezeichnung der Norm 3166 der Internationalen

Dimension	Beschreibung
	<p>Organisation für Normung (ISO). Zum Beispiel US für die Vereinigten Staaten und UA für die Ukraine.</p> <p>Wenn eine Anfrage einen X-Forwarded-For Header hat, AWS WAF verwendet diesen, um diese Einstellung zu bestimmen. Andernfalls AWS WAF wird das Land der Client-IP verwendet. Diese Bestimmung ist unabhängig von der Logik, die Sie in Ihren Regeln verwenden, um das Herkunftsland zu bestimmen. AWS WAF bestimmt die Standorte der IPs mithilfe von MaxMind GeoIP-Datenbanken.</p>
Attack	<p>Die Art des Angriffs, der in der Anfrage AWS WAF identifiziert wurde, basierend auf den Regeln und Regelgruppen, die Sie in Ihrer Web-ACL verwenden.</p> <p>Anhand Ihrer Regeln und der Regeln in den AWS verwalteten Basisregelgruppen können Sie Angriffstypen identifizieren. Beispielsweise identifizieren Cross-Site Scripting (XSS) -Regelabgleiche XSS-Angriffstypen, und ratenbasierte Regeln identifizieren volumetrische Angriffstypen. Der Angriffstyp gibt in der Regel den Regeltyp an, durch den die Auswertung der Webanforderung beendet wurde.</p>
Device	<p>Der Gerätetyp des Clients, der die Anfrage gesendet hat. Er wird aus dem user-agent Header der Webanfrage abgerufen.</p>
ManagedRuleGroup	<p>Der Metrikname der verwalteten Regelgruppe, deren Regel die Auswertung der Webanfrage beendet hat.</p>

Kennzeichnen Sie Metriken und Dimensionen

Metriken für die Labels, die Anfragen während der Bewertung anhand Ihrer Regeln und der verwalteten Regelgruppen, die Sie in Ihrer Web-ACL verwenden, hinzugefügt wurden. Weitere Informationen finden Sie unter [Bezeichnungen bei Webanforderungen](#).

AWS WAF Speichert für jede einzelne Webanfrage Metriken für maximal 100 Labels. Ihre Web-ACL-Bewertung kann mehr als 100 Labels anwenden und mit mehr als 100 Labels abgleichen, aber nur die ersten 100 werden in den Metriken berücksichtigt.

Metriken kennzeichnen

Metrik	Beschreibung
AllowedRequests	<p>Die Anzahl der Labels in Webanfragen, auf die die Aktionseinstellung Allow angewendet wurde. Die Labels können zu einem beliebigen Zeitpunkt während der Auswertung der Webanfrage hinzugefügt worden sein.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Gültige Statistiken: Summe</p>
BlockedRequests	<p>Die Anzahl der Labels in Webanfragen, auf die die Aktionseinstellung Block angewendet wurde. Die Labels können zu einem beliebigen Zeitpunkt während der Auswertung der Webanfrage hinzugefügt worden sein.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Gültige Statistiken: Summe</p>
CountedRequests	<p>Die Anzahl der Labels, die Webanfragen durch Regelgruppenregeln mit einer Count Aktionseinstellung hinzugefügt wurden.</p> <p>Diese Metrik steht nur dem Besitzer einer Regelgruppe für Regeln innerhalb der Regelgruppe zur Verfügung. In anderen Fällen werden die Metriken</p>

Metrik	Beschreibung
	<p>für die Zählmarkierung in der abschließenden Aktion zusammengefasst, die auf die Anfrage angewendet wurde, z. B. Allow oder Block.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Gültige Statistiken: Summe</p>
CaptchaRequests	<p>Die Anzahl der Labels in Webanfragen, auf die eine abschließende CAPTCHA Aktion angewendet wurde. Die Labels können zu einem beliebigen Zeitpunkt während der Auswertung der Webanfrage hinzugefügt worden sein.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Gültige Statistiken: Summe</p>
ChallengeRequests	<p>Die Anzahl der Labels auf Webanfragen, auf die eine abschließende Challenge Aktion angewendet wurde. Die Labels können zu einem beliebigen Zeitpunkt während der Auswertung der Webanfrage hinzugefügt worden sein.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Gültige Statistiken: Summe</p>

Abmessungen des Etiketts

Dimension	Beschreibung
Region	Erforderlich für alle geschützten Ressourcentypen außer für CloudFront Amazon-Distributionen.
WebACL	Der Metrikname der WebACL.

Dimension	Beschreibung
RuleGroup	Der Metrikname der RuleGroup . Wird für die Metrik CountedRequests verwendet.
LabelNamespace	Das Namespace-Präfix des Labels, das der Anfrage hinzugefügt wurde.
Label	Der Name des Labels, das der Anfrage hinzugefügt wurde.
Context	Die verwaltete Regelgruppe, die als Kontext für das Hinzufügen des Labels diente. Der Kontext für Token-Management-Bezeichnungen wie z. B. <code>awsaf:managed:token:accepted</code> ist die AWS WAF verwaltete Regelgruppe, die Tokenverwaltung für die Anfrage verwendet, wie z. B. die von Bot Control oder ATP verwaltete Regelgruppe. Diese Dimension gilt nicht für alle Labels.

Kostenlose Messwerte und Dimensionen zur Bot-Sichtbarkeit

Wenn Sie Bot Control nicht in Ihrer Web-ACL verwenden, AWS WAF wendet die von Bot Control verwaltete Regelgruppe ohne zusätzliche Kosten auf eine Stichprobe Ihrer Webanfragen an. Auf diese Weise können Sie sich ein Bild vom Bot-Traffic machen, der auf Ihre geschützten Ressourcen gelangt. Informationen zu Bot Control finden Sie unter [AWS WAF Regelgruppe „Bot-Kontrolle“](#).

Kostenlose Messwerte zur Bot-Sichtbarkeit

Metrik	Beschreibung
SampleAllowedRequest	Die Anzahl der in die Stichprobe einbezogenen Anfragen, für die es eine Allow Aktion gibt. Berichtskriterien: Ein Wert ungleich Null. Gültige Statistiken: Summe

Metrik	Beschreibung
SampleBlockedRequest	Die Anzahl der in die Stichprobe einbezogenen Anfragen, für die eine Aktion ausgeführt wurdeBlock. Berichtskriterien: Ein Wert ungleich Null. Gültige Statistiken: Summe
SampleCaptchaRequest	Die Anzahl der in die Stichprobe einbezogenen Anfragen, für die eine Aktion ausgeführt wurdeCAPTCHA. Berichtskriterien: Ein Wert ungleich Null. Gültige Statistiken: Summe
SampleChallengeRequest	Die Anzahl der in die Stichprobe einbezogenen Anfragen, für die eine Aktion ausgeführt wurdeChallenge. Berichtskriterien: Ein Wert ungleich Null. Gültige Statistiken: Summe
SampleCountRequest	Die Anzahl der in die Stichprobe einbezogenen Anfragen, für die eine Aktion ausgeführt wurdeCount. Berichtskriterien: Ein Wert ungleich Null. Gültige Statistiken: Summe

Kostenlose Abmessungen für die Sichtbarkeit von Bots

Dimension	Beschreibung
Region	Erforderlich für alle geschützten Ressourcentypen außer für CloudFront Amazon-Distributionen.
WebACL	Der Metrikname der WebACL.

Dimension	Beschreibung
BotCategory	Der Name der erkannten Bot-Kategorie, basierend auf den Labels der Webanforderung.
VerificationStatus	Der Name des Bestätigungsstatus des erkannten Bots, basierend auf den Labels für die Webanfrage.
Signal	Der Name der erkannten Bot-Signale, basierend auf den Labels für die Webanforderung.

AWS Shield Advanced Metriken

Shield Advanced veröffentlicht Statistiken zur CloudWatch Erkennung und Abwehr von Amazon und zu den wichtigsten Mitwirkenden für alle Ressourcen, die es schützt. Diese Kennzahlen verbessern Ihre Fähigkeit, Ihre Ressourcen zu überwachen, indem sie es ermöglichen, CloudWatch Dashboards und Alarme für sie zu erstellen und zu konfigurieren.

Die Shield Advanced-Konsole präsentiert Zusammenfassungen vieler der von ihr aufgezeichneten Metriken. Weitere Informationen finden Sie unter [Einblick in DDoS-Ereignisse](#).

Wenn Sie die automatische DDoS-Abwehr auf Anwendungsebene für den Schutz auf Anwendungsebene aktivieren,

Standorte für die Berichterstattung anhand von Kennzahlen

Shield Advanced meldet Kennzahlen für die Region USA Ost (Nord-Virginia) us-east-1 für Folgendes:

- Die globalen Dienste Amazon CloudFront und Amazon Route 53.
- Schutzgruppen. Informationen zu Schutzgruppen finden Sie unter [AWS Shield Advanced Schutzgruppen](#).

Für andere Ressourcentypen meldet Shield Advanced Metriken in der Region der Ressource.

Zeitpunkt der Metrikberichterstattung

Shield Advanced meldet CloudWatch Amazon bei DDoS-Ereignissen häufiger Kennzahlen zu einer AWS Ressource als zu Zeiten, in denen keine Ereignisse im Gange sind. Shield Advanced meldet

Metriken einmal pro Minute während eines Ereignisses und dann einmal direkt nach dem Ende des Ereignisses.

Solange keine Ereignisse im Gange sind, meldet Shield Advanced Metriken einmal täglich zu einer der Ressource zugewiesenen Zeit. Durch diesen regelmäßigen Bericht bleiben die Messwerte aktiv und können in benutzerdefinierten CloudWatch Alarmen und Dashboards verwendet werden.

Empfehlungen für Alarme

Wir empfehlen Ihnen, Alarme einzurichten, um Sie über Umstände zu informieren, die Ihre Aufmerksamkeit erfordern. Als Ausgangspunkt könnten Sie für jede geschützte Ressource einen Alarm erstellen, der meldet, wenn die `DDoSDetected` Erkennungsmetrik ungleich Null ist. Ein Wert ungleich Null in dieser Metrik bedeutet nicht unbedingt, dass ein DDoS-Angriff im Gange ist. Wir empfehlen jedoch, den Ressourcenstatus genauer zu untersuchen, wenn sich die Metrik in diesem Status befindet.

Bei einer Flut von Anfragen empfehlen wir, Alarme für kombinierte Prüfungen zu erstellen, bei denen auch Faktoren wie der Zustand der Anwendung und das Volumen der Webanfragen berücksichtigt werden. Sie können sich dafür entscheiden, den Alarm anhand der anderen drei Messwerte zu aktivieren, die das Datenverkehrsvolumen für verschiedene Angriffsvektor-Dimensionen angeben. Indem Sie die Kapazität Ihrer Anwendung berücksichtigen und Sie alarmieren, wenn sich der Datenverkehr Ihren Anwendungsbeschränkungen nähert, können Sie eine Reihe von Regeln erstellen, die Sie bei Bedarf benachrichtigen, ohne dass zu viel unerwünschtes Rauschen entsteht.

Themen

- [Erkennungsmetriken](#)
- [Kennzahlen zur Schadensbegrenzung](#)
- [Kennzahlen der wichtigsten Mitwirkenden](#)

Erkennungsmetriken

Shield Advanced stellt die Metriken und Dimensionen im `AWS/DDoSProtection` Namespace bereit.

Erkennungsmetriken

Metrik	Beschreibung
<code>DDoSDetected</code>	<p>Gibt an, ob ein DDoS-Ereignis für einen bestimmten Amazon Resource Name (ARN) stattfindet.</p> <p>Diese Metrik hat während eines Ereignisses einen Wert ungleich Null.</p>
<code>DDoSAttackBitsPerSecond</code>	<p>Die Anzahl an Bits, die während eines DDoS-Ereignisses für einen bestimmten Amazon-Ressourcennamen (ARN) erfasst wurden. Diese Metrik ist nur für DDoS-Ereignisse auf Netzwerk- und Transportschicht (Layer 3 und Layer 4) verfügbar.</p> <p>Diese Metrik hat während eines Ereignisses einen Wert ungleich Null.</p> <p>Einheiten: Bits</p>
<code>DDoSAttackPacketsPerSecond</code>	<p>Die Anzahl an Paketen, die während eines DDoS-Ereignisses für einen bestimmten Amazon-Ressourcennamen (ARN) erfasst wurden. Diese Metrik ist nur für DDoS-Ereignisse auf Netzwerk- und Transportschicht (Layer 3 und Layer 4) verfügbar.</p> <p>Diese Metrik hat während eines Ereignisses einen Wert ungleich Null.</p> <p>Einheiten: Pakete</p>
<code>DDoSAttackRequestsPerSecond</code>	<p>Die Anzahl an Abfragen, die während eines DDoS-Ereignisses für einen bestimmten Amazon-Ressourcennamen (ARN) erfasst wurden. Diese Metrik ist nur für Layer 7-DDoS-</p>

Metrik	Beschreibung
	<p>Ereignisse verfügbar. Diese Metrik wird nur für die wichtigsten Layer 7-Ereignisse gemeldet.</p> <p>Diese Metrik hat während eines Ereignisses einen Wert ungleich Null.</p> <p>Einheiten: Abfragen</p>

Shield Advanced veröffentlicht die DDoSDetected Metrik ohne andere Dimensionen. Die verbleibenden Erkennungsmetriken umfassen die AttackVector Dimensionen, die der Art des Angriffs entsprechen, aus der folgenden Liste:

- ACKFlood
- ChargenReflection
- DNSReflection
- GenericUDPReflection
- MemcachedReflection
- MSSQLReflection
- NetBIOSReflection
- NTPReflection
- PortMapper
- RequestFlood
- RIPReflection
- SNMPReflection
- SSDPReflection
- SYNflood
- UDPFragment
- UDPTraffic
- UDPReflection

Kennzahlen zur Schadensbegrenzung

Shield Advanced stellt Metriken und Dimensionen im `AWS/DDoSProtection` Namespace bereit.

Metriken zur Risikominderung

Metrik	Beschreibung
<code>VolumePacketsPerSecond</code>	Die Anzahl der Pakete pro Sekunde, die im Rahmen einer Schadensbegrenzung, die als Reaktion auf ein erkanntes Ereignis eingesetzt wurde, verworfen oder weitergeleitet wurden. Einheiten: Pakete

Dimensionen der Schadensbegrenzung

Dimension	Beschreibung
<code>ResourceArn</code>	Amazon-Ressourcenname (ARN)
<code>MitigationAction</code>	Das Ergebnis einer angewandten Schadensbegrenzung. Die möglichen Wert sind <code>Pass</code> oder <code>Drop</code> .

Kennzahlen der wichtigsten Mitwirkenden

Shield Advanced stellt Metriken im `AWS/DDoSProtection` Namespace bereit.

Metriken der wichtigsten Mitwirkenden

Metrik	Beschreibung
<code>VolumePacketsPerSecond</code>	Die Anzahl der Pakete pro Sekunde für einen Top-Beitragenden. Einheiten: Pakete
<code>VolumeBitsPerSecond</code>	Die Anzahl der Bits pro Sekunde für einen Top-Beitragenden.

Metrik	Beschreibung
	Einheiten: Bits

Shield Advanced veröffentlicht Kennzahlen zu den wichtigsten Mitwirkenden nach Dimensionskombinationen, die die Mitwirkenden der Veranstaltung charakterisieren. Sie können jede der folgenden Kombinationen von Dimensionen für alle Kennzahlen der wichtigsten Mitwirkenden verwenden:

- ResourceArn, Protocol
- ResourceArn, Protocol, SourcePort
- ResourceArn, Protocol, DestinationPort
- ResourceArn, Protocol, SourceIp
- ResourceArn, Protocol, SourceAsn
- ResourceArn, TcpFlags

Dimensionen der wichtigsten Mitwirkenden

Dimension	Beschreibung
ResourceArn	Amazon-Ressourcenname (ARN).
Protocol	IP-Protokollname, entweder TCP oder UDP.
SourcePort	Quell-TCP- oder UDP-Port.
DestinationPort	Ziel-TCP- oder UDP-Port.
SourceIp	Quell-IP-Adresse.
SourceAsn	Nummer des autonomen Quellsystems (ASN).
TcpFlags	Eine Kombination von Flags, die in einem TCP-Paket vorhanden sind und durch einen Bindestrich (-) getrennt sind. Überwachte Flags sind ACKFIN,,RST,SYN. Dieser Dimensionswert wird

Dimension	Beschreibung
	immer alphabetisch sortiert angezeigt. Beispiel: ACK-FIN-RST-SYN , ACK-SYN und FIN-RST.

AWS Firewall Manager Benachrichtigungen

AWS Firewall Manager zeichnet keine Metriken auf, sodass Sie keine CloudWatch Amazon-Alarme speziell für Firewall Manager erstellen können. Sie können jedoch Amazon SNS SNS-Benachrichtigungen so konfigurieren, dass sie Sie vor potenziellen Angriffen warnen. Informationen zum Erstellen von Amazon SNS SNS-Benachrichtigungen in Firewall Manager finden Sie unter [Schritt 4: Amazon SNS SNS-Benachrichtigungen und CloudWatch Amazon-Alarme konfigurieren](#).

Protokollierung von AWS CloudTrail-API-Aufrufen mit

AWS WAF AWS Shield Advanced, und AWS Firewall Manager sind in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS Dienst ausgeführten Aktionen bereitstellt. CloudTrail erfasst eine Teilmenge der API-Aufrufe für diese Dienste als Ereignisse, einschließlich Aufrufe von den AWS WAF Shield Advanced- oder Firewall Manager Manager-Konsolen und von Codeaufrufen an die AWS WAF Shield Advanced- oder Firewall Manager Manager-APIs. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für AWS WAF Shield Advanced oder Firewall Manager. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an diese Dienste gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen darüber CloudTrail, einschließlich der Konfiguration und Aktivierung, finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn unterstützte Ereignisaktivitäten in AWS WAF Shield Advanced oder Firewall Manager auftreten, wird diese Aktivität zusammen mit anderen AWS Dienstereignissen im CloudTrail Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter [Ereignisse mit CloudTrail Ereignisverlauf anzeigen](#).

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich Ereignissen für AWS WAF Shield Advanced oder Firewall Manager, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Standardmäßig gilt ein in der Konsole erstellter Trail für alle Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail Unterstützte Dienste und Integrationen](#)
- [Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#)

AWS WAF Informationen in AWS CloudTrail

Alle AWS WAF Aktionen werden von der [AWS WAF API-Referenz](#) protokolliert AWS CloudTrail und sind in dieser dokumentiert. Zum Beispiel Aufrufe von `ListWebACLUpdateWebACL`, und `DeleteWebACL` generieren Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root-Benutzeranmeldedaten gestellt wurde
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde

Weitere Informationen finden Sie unter [CloudTrailUserIdentity](#) Element.

Beispiel: AWS WAF Einträge in Protokolldateien

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. AWS CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das

Datum und die Uhrzeit der Aktion sowie über die Anforderungsparameter. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge erscheinen.

Im Folgenden finden CloudTrail Sie Beispiele für Protokolleinträge für AWS WAF Web-ACL-Operationen.

Beispiel: CloudTrail Protokolleintrag für 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": "ebbc976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "description": "foo",
    "lockToken": "67551e73-49d8-4363-be48-244deea72ea9",
    "aRN": "arn:aws:wafv2:us-east-1:112233445566:global/webacl/foo/
ebbc976-8d59-4d20-8ca8-4ab2f6b7c07b"
  }
},
"requestID": "c51521ba-3911-45ca-ba77-43aba50471ca",
"eventID": "afd1a60a-7d84-417f-bc9c-7116cf029065",
"eventType": "AwsApiCall",

```

```
"apiVersion": "2019-04-23",  
"recipientAccountId": "112233445566"  
}
```

Beispiel: CloudTrail Protokolleintrag für 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"
}

```

Beispiel: CloudTrail Protokolleintrag für 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": "ebbc976-8d59-4d20-8ca8-4ab2f6b7c07b",

```

```
"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"
}
```

Beispiel: CloudTrail Protokolleintrag für 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": "ebbc976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "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"
}
```

Beispiel: AWS WAF klassische Logdateieinträge

AWS WAF Classic ist die vorherige Version von AWS WAF. Weitere Informationen finden Sie unter [AWS WAF Klassisch](#).

Der Protokolleintrag zeigt die Operationen CreateRule, GetRule, UpdateRule und 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": "19434322-8685-4ed2-9c5b-9410bexample",
        "metricName": "0923ab32722949f0a0e366c81example"
      },
      "responseElements": {
        "rule": {
          "metricName": "0923ab32722949f0a0e366c81example",
          "ruleId": "12132e64-6750-4725-b714-e7544example",
          "predicates": [

          ],
          "name": "0923ab32-7229-49f0-a0e3-66c81example"
        },
        "changeToken": "19434322-8685-4ed2-9c5b-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 Informationen in CloudTrail

AWS Shield Advanced unterstützt die Protokollierung der folgenden Aktionen als Ereignisse in CloudTrail Protokolldateien:

- [ListAttacks](#)
- [DescribeAttack](#)
- [CreateProtection](#)
- [DescribeProtection](#)
- [DeleteProtection](#)
- [ListProtections](#)
- [CreateSubscription](#)
- [DescribeSubscription](#)
- [GetSubscriptionState](#)

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root-Benutzeranmeldedaten gestellt wurde
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter dem [CloudTrail UserIdentity-Element](#).

Beispiel: Shield Advanced-Protokolldateieinträge

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `ListProtections` Aktionen `DeleteProtection` und demonstriert.

```
[
  {
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "1234567890987654321231",
      "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 Informationen in CloudTrail

AWS Firewall Manager unterstützt die Protokollierung der folgenden Aktionen als Ereignisse in CloudTrail Protokolldateien:

- [AssociateAdminAccount](#)
- [DeleteNotificationChannel](#)
- [DeletePolicy](#)
- [DisassociateAdminAccount](#)
- [PutNotificationChannel](#)
- [PutPolicy](#)
- [GetAdminAccount](#)
- [GetComplianceDetail](#)
- [GetNotificationChannel](#)

- [GetPolicy](#)
- [ListComplianceStatus](#)
- [ListPolicies](#)

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root-Benutzeranmeldedaten gestellt wurde
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter dem [CloudTrail UserIdentity-Element](#).

Beispiel: Einträge in der Firewall Manager Manager-Protokolldatei

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die Aktion GetAdminAccount --> demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "1234567890987654321231",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/SampleUser",
    "accountId": "123456789012",
    "accessKeyId": "1AFGDT647FHU83JHFI81H",
    "sessionContext": {
      "attributes": {
```

```

"false",
"2018-04-14T02:51:50Z"
"1234567890987654321231",
"arn:aws:iam::123456789012:role/Admin",
"123456789012",
    "mfaAuthenticated":
    "creationDate":
    },
    "sessionIssuer": {
        "type": "Role",
        "principalId":
        "arn":
        "accountId":
        "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"
}

```

Verwenden der AWS WAFAWS Shield Advanced and-API

In diesem Abschnitt wird beschrieben, wie Sie Anfragen an die AWS WAF Shield Advanced-API zur Erstellung und Verwaltung von Matchsätzen, Regeln und Web-ACLs AWS WAF sowie an Ihr Abonnement und Ihre Schutzmaßnahmen in Shield Advanced stellen. Sie lernen in diesem Abschnitt die Komponenten der Anforderungen, die Inhalte der Antworten und die Authentifizierung von Anforderungen kennen.

Themen

- [Verwendung der AWS SDKs](#)
- [HTTPS-Anfragen an AWS WAF oder Shield Advanced stellen](#)
- [HTTP-Antworten](#)
- [Authentifizieren von Anforderungen](#)

Verwendung der AWS SDKs

Wenn Sie eine Sprache verwenden, für die AWS ein SDK bereitgestellt wird, verwenden Sie das SDK, anstatt zu versuchen, sich durch die APIs zu arbeiten. Die SDKs vereinfachen die Authentifizierung, lassen sich problemlos in Ihre Entwicklungsumgebung integrieren und bieten einfachen Zugriff auf Shield Advanced-Befehle AWS WAF und Shield Advanced-Befehle. Weitere Informationen zu den AWS SDKs finden Sie [Tools herunterladen](#) im Thema [Einrichtung](#)

HTTPS-Anfragen an AWS WAF oder Shield Advanced stellen

AWS WAF und Shield Advanced-Anfragen sind HTTPS-Anfragen, wie in [RFC 2616](#) definiert. Wie jede HTTP-Anfrage enthält eine Anfrage an AWS WAF oder Shield Advanced eine Anforderungsmethode, einen URI, Anforderungsheader und einen Anforderungstext. Die Antwort enthält einen HTTP-Statuscode, Antwort-Header und manchmal auch Antworttext.

Anforderungs-URI

Die Anforderungs-URI ist immer ein einzelner Schrägstrich /.

HTTP-Header

AWS WAF und Shield Advanced benötigen die folgenden Informationen im Header einer HTTP-Anfrage:

Host (erforderlich)

Dieser Endpunkt gibt an, wo die Ressourcen erstellt werden. Informationen zu Endpunkten finden Sie unter [AWS Dienstendpunkte](#). Der Wert der Host Kopfzeile für eine CloudFront Verteilung ist AWS WAF beispielsweise `waf.amazonaws.com:443`

x-amz-date oder Datum (erforderlich)

Das Datum, an dem die im Header `Authorization` enthaltene Signatur erstellt wurde. Geben Sie das Datum wie folgt im ISO 8601-Standardformat in UTC-Zeit an:

```
x-amz-date: 20151007T174952Z
```

Sie müssen entweder `x-amz-date` oder `Date` angeben. (Einige HTTP-Client-Bibliotheken lassen den Header `Date` nicht zu). Wenn ein `x-amz-date` Header vorhanden ist, werden alle `Date` Header bei der Authentifizierung der Anfrage AWS WAF ignoriert.

Der Zeitstempel muss innerhalb von 15 Minuten nach der AWS Systemzeit liegen, zu der die Anfrage eingegangen ist. Ist das nicht der Fall, schlägt die Anforderung mit dem Fehlercode `RequestExpired` fehl, damit niemand sonst Ihre Anforderungen wiedergeben kann.

Autorisierung (erforderlich)

Die erforderlichen Informationen für die Anforderungsauthentifizierung. Weitere Informationen zum Erstellen dieses Headers finden Sie unter [Authentifizieren von Anforderungen](#).

X-Amz-Ziel (erforderlich)

Eine Kombination aus `AWSWAF_` oder `AWSShield_`, der API-Version ohne Zeichensetzung, einem Punkt (.) und dem Vorgangsnamen, z. B.:

```
AWSWAF_20150824.CreateWebACL
```

Content-Type (bedingt)

Gibt als Inhaltstyp JSON sowie die JSON-Version an, z. B.:

```
Content-Type: application/x-amz-json-1.1
```

Bedingung: Für POST Anfragen erforderlich.

Content-Length (bedingt)

Länge der Nachricht (ohne Header) gemäß RFC 2616.

Bedingung: Erforderlich, wenn der Anforderungstext selbst Informationen enthält (die meisten Toolkits fügen diesen Header automatisch hinzu).

Nachfolgend finden Sie einen Beispiel-Header für eine HTTP-Anforderung zum Erstellen einer Web-ACL in 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
```

HTTP-Anforderungstext

Bei vielen AWS WAF und Shield Advanced API-Aktionen müssen Sie Daten im JSON-Format in den Hauptteil der Anfrage aufnehmen.

Die folgende Beispielanforderung verwendet eine einfache JSON-Anweisung, um eine so zu aktualisieren, dass sie die IP-Adresse 192.0.2.44 (in der CIDR-Notation als 192.0.2.44/32 dargestellt) enthält: IPSet

```
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"
      }
    }
  ]
}
```

HTTP-Antworten

Alle API-Aktionen AWS WAF und Shield Advanced beinhalten Daten im JSON-Format in der Antwort.

Nachfolgend werden einige wichtige Header in der HTTP-Antwort und der Umgang mit diesen in der Anwendung (sofern verwendet) erläutert:

HTTP/1.1

Diesem Header folgt ein Statuscode. Der Statuscode 200 gibt an, dass der Vorgang erfolgreich war.

Typ: Zeichenfolge

x-amzn- RequestId

Ein von AWS WAF oder Shield Advanced erstellter Wert, der Ihre Anfrage eindeutig identifiziert, K2QH8DN0U907N97FNA2GDLL80BVV4KQNS05AEMVJF66Q9ASUAAJG z. B. Wenn Sie ein Problem mit haben AWS WAF, AWS können Sie diesen Wert verwenden, um das Problem zu beheben.

Typ: Zeichenfolge

Content-Length

Die Länge des Antworttexts in Byte.

Typ: Zeichenfolge

Datum

Das Datum und die Uhrzeit, zu der AWS WAF oder Shield Advanced geantwortet haben, z. B. Mittwoch, 07. Oktober 2015 12:00:00 Uhr GMT.

Typ: Zeichenfolge

Fehlermeldungen

Falls eine Anforderung fehlschlägt, enthält die HTTP-Antwort folgende Werte:

- Ein JSON-Fehlerdokument als Antworttext
- Content-Type
- Den zutreffenden 3xx, 4xx oder 5xx HTTP-Statuscode

Hier finden Sie ein Beispiel für ein JSON-Fehlerdokument:

```
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"}
```

Authentifizieren von Anforderungen

Wenn Sie eine Sprache verwenden, für die AWS ein SDK bereitgestellt wird, empfehlen wir Ihnen, das SDK zu verwenden. Alle AWS SDKs vereinfachen das Signieren von Anfragen erheblich und sparen Ihnen viel Zeit im Vergleich zur Verwendung der AWS WAF oder Shield Advanced-API.

Darüber hinaus lassen sich die SDKs leicht in die Entwicklungsumgebung integrieren und bieten einen einfachen Zugriff auf zugehörige Befehle.

AWS WAF und Shield Advanced verlangen, dass Sie jede Anfrage, die Sie senden, authentifizieren, indem Sie die Anfrage signieren. Zum Signieren einer Anforderung berechnen Sie eine digitale Signatur mithilfe einer kryptografischen Hash-Funktion, die einen Hash-Wert basierend auf der Eingabe zurückgibt. Die Eingabe umfasst den Text der Anforderung und den geheimen Zugriffsschlüssel. Die Hash-Funktion gibt einen Hash-Wert zurück, den Sie in die Anforderung als Ihre Signatur einfügen. Die Signatur ist Teil des Headers `Authorization` in der Anforderung.

Nach Erhalt Ihrer Anfrage berechnet Shield Advanced die Signatur mit derselben Hash-Funktion und Eingabe neu, mit der Sie die Anfrage signiert haben. AWS WAF Wenn die resultierende Signatur mit der Signatur in der Anfrage übereinstimmt AWS WAF oder Shield Advanced die Anfrage verarbeitet. Andernfalls wird die Anforderung abgelehnt.

AWS WAF und Shield Advanced unterstützt die Authentifizierung mit [AWS Signature Version 4](#). Der Prozess zum Berechnen einer Signatur lässt sich in drei Aufgaben untergliedern:

[Aufgabe 1: Erstellen einer kanonischen Anforderung](#)

Erstellen Sie die HTTP-Anforderung im kanonischen Format, wie unter [Aufgabe 1: Erstellen einer kanonischen Anforderung für Signature Version 4](#) in der Allgemeine Amazon Web Services-Referenz beschrieben.

[Aufgabe 2: Erstellen einer zu signierenden Zeichenfolge](#)

Erstellen Sie eine Zeichenfolge, die Sie als einen der Eingabewerte für die kryptografische Hash-Funktion nutzen. Die Zeichenfolge – auch als zu signierende Zeichenfolge bezeichnet – ist eine Kombination aus den folgenden Werten:

- Name des Hash-Algorithmus
- Anforderungsdatum
- Zeichenfolge mit dem Umfang der Anmeldeinformationen
- Kanonische Anforderung aus der vorigen Aufgabe

Die Zeichenfolge mit dem Umfang der Anmeldeinformationen selbst ist eine Kombination aus Datum, Region und Serviceinformationen.

Geben Sie Folgendes für den Parameter `X-Amz-Credential` an:

- Code für den Endpunkt, an den Sie die Anforderung senden, `us-east-2`.

- waf für das Servicekürzel

Beispielsweise:

```
X-Amz-Credential=AKIAIOSFODNN7EXAMPLE/20130501/us-east-2/waf/  
aws4_request
```

Aufgabe 3: Erstellen einer Signatur

Erstellen Sie mithilfe einer kryptografischen Hash-Funktion, die zwei Eingabezeichenfolgen akzeptiert, eine Signatur für Ihre Anforderung:

- Die zu signierende Zeichenfolge aus Aufgabe 2
- Einen abgeleiteten Schlüssel Der abgeleitete Schlüssel wird unter Nutzung des geheimen Zugriffsschlüssels und der Zeichenfolge mit dem Umfang der Anmeldeinformationen berechnet, um eine Reihe von Hash-Nachrichtenauthentifizierungscodes (Hashed Message Authentication Code, HMAC) zu erstellen.

Ähnliche Informationen

Die folgenden verwandten Ressourcen bieten Ihnen nützliche Informationen für die Arbeit mit diesem Service.

Die folgenden Ressourcen sind für AWS WAF AWS Shield Advanced, und verfügbar AWS Firewall Manager.

- [Richtlinien für die Implementierung AWS WAF](#) — Technische Publikation mit aktuellen Implementierungsempfehlungen AWS WAF zum Schutz vorhandener und neuer Webanwendungen.
- [AWS Diskussionsforen](#) — Ein Community-Forum zur Erörterung technischer Fragen zu diesem und anderen AWS Diensten.
- [AWS WAF Diskussionsforum](#) — Ein Community-Forum für Entwickler zur Diskussion technischer Fragen im Zusammenhang mit AWS WAF
- [Shield-Advanced-Diskussionsforum](#): Ein Community-basiertes Forum für Entwickler, um über technische Fragen zu Shield Advanced zu diskutieren.
- [AWS WAF Produktinformationen](#) — Die wichtigste Webseite mit Informationen zu Funktionen AWS WAF, Preisen und mehr.
- [Produktinformationen zu Shield Advanced](#): Die Hauptwebseite für Informationen zu Shield Advanced mit Funktionen, Preisen und mehr.

Die folgenden Ressourcen sind für Amazon Web Services verfügbar.

- [Kurse und Workshops](#) — Links zu rollen- und Spezialkursen sowie zu Übungen zum Selbststudium, mit denen Sie Ihre AWS Fähigkeiten verbessern und praktische Erfahrungen sammeln können.
- [AWS Developer Center](#) — Erkunden Sie Tutorials, laden Sie Tools herunter und erfahren Sie mehr über Veranstaltungen für Entwickler. AWS
- [AWS Entwicklertools](#) — Links zu Entwicklertools, SDKs, IDE-Toolkits und Befehlszeilentools für die Entwicklung und Verwaltung von AWS Anwendungen.
- [Ressourcencenter für die ersten Schritte](#) — Erfahren Sie, wie Sie Ihre AWS-Konto Anwendung einrichten, der AWS Community beitreten und Ihre erste Anwendung starten.
- [Praktische Tutorials](#) — Folgen Sie den step-by-step Tutorials, um Ihre erste Anwendung zu starten. AWS

- [AWS Whitepapers](#) — Links zu einer umfassenden Liste von technischen AWS Whitepapers zu Themen wie Architektur, Sicherheit und Wirtschaft, die von Solutions Architects oder anderen technischen Experten verfasst wurden. AWS
- [AWS Support Center](#) — Die zentrale Anlaufstelle für die Erstellung und Verwaltung Ihrer Fälle. AWS Support Enthält auch Links zu anderen hilfreichen Ressourcen wie Foren, häufig gestellten Fragen zu technischen Fragen, dem Status des Dienstes und AWS Trusted Advisor.
- [AWS Support](#) — Die wichtigste Webseite mit Informationen über AWS Support einen Support-Kanal mit schnellen Reaktionszeiten one-on-one, der Sie bei der Entwicklung und Ausführung von Anwendungen in der Cloud unterstützt.
- [Kontakt](#) — Zentraler Kontaktpunkt für Fragen zu AWS -Abrechnung, Konten, Ereignissen Missbrauch und anderen Problemen.
- [AWS Nutzungsbedingungen der Website](#) — Detaillierte Informationen zu unseren Urheberrechten und Marken, zu Ihrem Konto, Ihrer Lizenz und Ihrem Zugriff auf die Website sowie zu anderen Themen.

Dokumentverlauf

Auf dieser Seite werden wichtige Änderungen an dieser Dokumentation aufgeführt.

Servicefunktionen werden manchmal schrittweise in den AWS Regionen eingeführt, in denen ein Dienst verfügbar ist. Wir aktualisieren diese Dokumentation nur für die erste Version. Wir stellen keine Informationen über die Verfügbarkeit von Regionen zur Verfügung und kündigen auch keine späteren Rollouts von Regionen an. Informationen zur regionalen Verfügbarkeit von Servicefunktionen und zum Abonnieren von Benachrichtigungen über Updates finden Sie unter [Was gibt's Neues bei AWS?](#) .

Änderung	Beschreibung	Datum
Updates für Firewall Manager Manager-Sicherheitsgruppenrichtlinien	Wir haben unsere Sicherheitsgruppenrichtlinien für Nutzungsaudits aktualisiert und die Dokumentation verbessert. Weitere Informationen finden Sie im Abschnitt Nutzungsüberwachungsrichtlinien und in den Abschnitten zu bewährten Methoden und Einschränkungen.	2. April 2024
Aktualisierte Beispiele für Bot-Kontrolle	Es wurden Beispiele hinzugefügt, die das angestrebte Inspektionsniveau veranschaulichen, und bestehende Beispiele wurden aktualisiert, um bewährte Verfahren widerzuspiegeln.	27. März 2024
Aktualisierte ATP-Beispiele	Es wurde ein Beispiel hinzugefügt, das die Konfiguration der Reaktionsinspektion zeigt, und bestehende Beispiele wurden aktualisiert	27. März 2024

	ert, um bewährte Verfahren widerzuspiegeln.	
Aktualisierte ACFP-Beispiele	Ein Beispiel zur Darstellung der Konfiguration von Response Inspection wurde hinzugefügt.	27. März 2024
Aktualisieren Sie die Beschränkungen für Amazon CloudWatch Logs Log-Streams	AWS WAF Es gibt keine webspezifischen ACL-Beschränkungen mehr für die Veröffentlichung von Protokollen in CloudWatch Logs-Log-Streams.	27. März 2024
AWS Shield Advanced Schutzmaßnahmen auf Anwendungsebene (Schicht 7)	Aktualisierte allgemeine und bewährte Leitlinien für die Erkennung und Abwehr von Anwendungsebenen, die Verwendung von Web-ACLs, ratenbasierte Regeln und automatische DDoS-Abwehr auf Anwendungsebene.	14. März 2024
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für die AWS WAF aktualisierte IP-Reputationsregelgruppe.	13. März 2024
Änderungen der Größenbeschränkungen für Körperinspektionen	AWS WAF unterstützt nun bei einigen regionalen Ressourcen größere Größenbeschränkungen für Körperinspektionen.	7. März 2024

<u>Konfigurierbares Bewertungsfenster für AWS WAF tarifbasierte Regeln</u>	Sie können jetzt das Zeitfenster, in dem ratenbasierte Regeln Anfragen zählen, auf 1, 2, 5 oder 10 Minuten konfigurieren. Die Standardinstellung ist 5, was vor dieser Version die einzige Option war.	28. Februar 2024
<u>Erweiterte Protokollierungsinformationen für CAPTCHA und Challenge</u>	Die oberste Ebene <code>captchaResponse</code> und die <code>challengeResponse</code> Felder sind jetzt mit den letzten dieser Aktionen gefüllt, die auf eine Anfrage angewendet werden sollen, unabhängig davon, ob sie beendet wurde oder nicht. Zuvor wurden diese Felder nur für die Beendigung von Aktionen ausgefüllt.	22. Februar 2024
<u>JavaScript CAPTCHA-API-Schlüsselverwaltung</u>	Sie können jetzt CAPTCHA JS-API-Schlüssel über die APIs löschen. AWS WAF	6. Februar 2024
<u>AWS WAF Audio für CAPTCHA-Rätsel</u>	Die Audioversion des CAPTCHA-Puzzles unterstützt jetzt mehrere Sprachen.	6. Februar 2024
<u>AWS WAF Kennzeichnung von Herausforderungen und CAPTCHA-Tokens</u>	Die Tokenverwaltung fügt jetzt Labels für das CAPTCHA-Token hinzu und hat die Token-Kennzeichnung für das Challenge-Token verbessert.	20. Dezember 2023

Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für haben die Regelgruppe „Bekannte fehlerhafte Eingaben“ AWS WAF aktualisiert.	16. Dezember 2023
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für haben die Regelgruppe „Bekannte fehlerhafte Eingaben“ AWS WAF aktualisiert.	14. Dezember 2023
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für die AWS WAF aktualisierte Regelgruppe des Kernregelsatzes (CRS).	6. Dezember 2023
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: AWS WAF Bot Control.	05. Dezember 2023
Aktualisierte AWS Config Voraussetzungen für Firewall Manager	Wenn Sie eine benutzerdefinierte IAM-Rolle anstelle der von Firewall Manager verwalteten Rolle für verwenden, müssen Sie sicherstellen AWS Config, dass Ihre Berechtigungsrichtlinie dem AWS Config Rekorder erlaubt, Firewall Manager Manager-Ressourcen aufzuzeichnen.	17. November 2023

AWS WAF Konsolen-Dashboards	Wir haben die Anleitung zur Anzeige aller Regeln und Musteranfragen für eine Web-ACL in der AWS WAF Konsole korrigiert.	17. November 2023
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für die AWS WAF Aktualisierung der Bot Control-Regelgruppe.	14. November 2023
AWS WAF Die Konsole hat neue Web-ACL-Dashboards	Die Web-ACL-Seite in der AWS WAF Konsole enthält neue Dashboards mit einer Übersicht über den Web-Traffic.	14. November 2023
Die von ATP verwaltete Regelgruppe wurde aktualisiert	Die Bezeichnungsinformationen für die Regeln VolumetricIpFailed LoginResponseHigh und wurden korrigiert VolumetricSessionFailedLoginResponseHigh .	13. November 2023
Die verwaltete ACFP-Regelgruppe wurde aktualisiert	Die Kennzeichnungsinformationen für die Regeln VolumetricIPSuccessfulResponse und VolumetricSessionSuccessfulResponse wurden korrigiert.	13. November 2023
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für die AWS WAF aktualisierte Regelgruppe des Kernregelsatzes (CRS).	2. November 2022

Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene	Shield Advanced verwaltet jetzt eine ratenbasierte Regel in der Regelgruppe zur automatischen Abwehr, die das Volumen der Anfragen von IP-Adressen begrenzt, von denen bekannt ist, dass sie Quellen von DDoS-Angriffen sind.	31. Oktober 2023
Aktualisierte verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für die AWS WAF aktualisierte Regelgruppe des Kernregelsatzes (CRS).	30. Oktober 2023
Die von Bot Control verwaltete Regelgruppe hat die Signalbezeichnung für die Anfrage CSP entfernt	Die von Bot Control verwaltete Regelgruppe hat die Signalbezeichnung entfernt, die den Clouddienstanbieter (CSP) angibt.	28. Oktober 2023
Die Signalbezeichnung der von Bot Control verwalteten Regelgruppe für die Anfrage CSP	Die Signalbeschriftungen der von Bot Control verwalteten Regelgruppen enthalten eine Bezeichnung, die den Cloud-Dienstanbieter (CSP) angibt.	27. Oktober 2023
Die Informationen zu den AWS WAF IAM-Berechtigungen wurden aktualisiert	Für die AWS WAF Aktionen, die Web-ACL-Verknüpfungen verwalten, werden im Abschnitt Richtlinienaktionen jetzt die Berechtigungsanforderungen für jeden Ressourcentyp für Webanwendungen aufgeführt.	25. Oktober 2023

Firewall Manager Manager-Verwaltung von modifizierten Web-ACLs	Wenn Sie die Verwaltung nicht zugeordneter Web-ACLs aktivieren, bezieht Firewall Manager die geänderten Web-ACLs nicht in die einmalige Bereinigung ungenutzter Ressourcen ein.	19. Oktober 2023
Aktualisierte verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für die AWS WAF aktualisierte Regelgruppe des POSIX-Betriebssystems, <code>AWSManagedRulesUnixRuleSet</code> .	12. Oktober 2023
AWS WAF Metriken hinzugefügte Dimensionen	AWS WAF neue Dimensionen für die Anzeige von Web-ACL-Metriken hinzugefügt.	12. Oktober 2023
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für die AWS WAF aktualisierte Regelgruppe des Kernregelsatzes (CRS).	11. Oktober 2023
Aktualisierung der SDK-Spezifikation AWS WAF für Mobilgeräte	Der <code>storeTokenInCookieStorage</code> Vorgang wurde hinzugefügt zu <code>WAFTokenProvider</code> .	11. Oktober 2023
Ausnahmebereitstellungen AWS Verwaltete Regeln für AWS WAF	AWS Managed Rules for AWS WAF hat zwei statische Versionen der Regelgruppe mit bekannten fehlerhaften Eingaben veröffentlicht und die Standardversion aktualisiert, sodass sie auf die neueste statische Version verweist.	04. Oktober 2023

<u>AWS WAF Umwandlung von Text in HTML-Entitäten dekodieren</u>	Die Funktionalität der Texttransformation zur Dekodierung von HTML-Entitäten wurde erweitert.	04. Oktober 2023
<u>Neue Option zur allgemeinen Richtlinie der Firewall Manager Manager-Sicherheitsgruppe hinzugefügt</u>	Firewall Manager kann jetzt Sicherheitsgruppenreferenzen an Replikatsicherheitsgruppen verteilen.	3. Oktober 2023
<u>AWS WAF fügt die Überprüfung des JA3-Fingerabdrucks hinzu</u>	Sie können jetzt einen exakten Abgleich mit dem JA3-Fingerabdruck der Webanfrage durchführen.	26. September 2023
<u>Aktualisierungen der Einstellungen der Sicherheitsgruppen richtlinienregeln von Firewall Manager</u>	Firewall Manager unterstützt jetzt die Referenzierung von Sicherheitsgruppen von primären Sicherheitsgruppen auf replizierte Sicherheitsgruppen.	25. September 2023
<u>Aktualisierte automatische DDoS-Abwehr auf Anwendungsebene von Shield Advanced</u>	Firewall Manager unterstützt jetzt Application Load Balancer Balancer-Ressourcen für Shield Advanced-Richtlinien, die mit automatischer DDoS-Abwehr auf Anwendungsebene konfiguriert sind.	14. September 2023
<u>Aktualisierte verwaltete Regeln AWS für AWS WAF</u>	AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: AWS WAF Bot Control.	6. September 2023

AWS WAF Bot-Steuerung	Die angestrebte Schutzstufe der von Bot Control verwalteten Regelgruppe überprüft nun die Wiederverwendung von Token zwischen IP-Adressen. Es bietet jetzt auch eine optionale maschinelle Lernanalyse von Verkehrsstatistiken, um einige Aktivitäten im Zusammenhang mit Bots zu erkennen.	6. September 2023
Aktualisierung der SDK-Spezifikation für Mobilgeräte AWS WAF	Die Min-, Max- und Standardwerte für <code>tokenRefreshDelaySec</code> wurden von min 300, max 600 und default 300 auf min 88, max 300 und default 88 gesenkt.	5. September 2023
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für die AWS WAF Aktualisierung der AWS WAF Bot Control-Regelgruppe.	30. August 2023
Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene	Es wurde eine Anleitung AWS CloudFormation zur Verwaltung der Web-ACLs hinzugefügt, die Sie mit automatischer DDoS-Abwehr auf Anwendungsebene verwenden.	30. August 2023
Neue Sicherheitsgruppenrichtlinienoption für die Inhaltsüberwachung in Firewall Manager	Es wurde eine neue Option für die Prüfung übermäßig freizügiger Regelgruppen und verbesserte Beschreibungen der Konsolenprozeduren hinzugefügt.	29. August 2023

<u>Neues Firewall Manager Manager-Schutzschild und neue AWS WAF Richtlinieoption</u>	Wenn Sie die Verwaltung nicht zugeordneter Web-ACLs in AWS WAF und Shield aktivieren, erstellt Firewall Manager nur dann Web-ACLs in den Konten innerhalb des Richtlinienbereichs, wenn die Web-ACLs von mindestens einer Ressource verwendet werden.	9. August 2023
<u>Aktualisierte verwaltete Regeln für AWS WAF</u>	AWS Verwaltete Regeln für die AWS WAF aktualisierte Regelgruppe des Kernregelsatzes (CRS).	26. Juli 2023
<u>Ratenbasierte Regelaggregation im URI-Pfad</u>	Sie können jetzt den URI-Pfad in Ihren benutzerdefinierten Aggregationsschlüsseln für ratenbasierte Regeln angeben.	19. Juli 2023
<u>Neue Option für AWS WAF Richtlinienregeln in AWS Firewall Manager</u>	AWS Firewall Manager fügt Unterstützung für die Konfiguration von Größenbeschränkungen für die Überprüfung von Textkörpern für AWS WAF Webanfragen hinzu.	18. Juli 2023

[AWS WAF verwaltete Richtlinienänderungen](#)

Die Ressourcentypen `AWSWAFFullAccessPolicy`, `AWSWAFConsoleFullAccess`, `AWSWAFReadOnlyAccess`, mit denen Sie `AWSWAFConsoleReadOnlyAccess` sich schützen können, wurden aktualisiert, und um „AWS Verifizierter Zugriff“ erweitert AWS WAF.

17. Juni 2023

[Aktualisierte AWS verwaltete Regeln für AWS WAF](#)

AWS Verwaltete Regeln für AWS WAF haben die Regelgruppe hinzugefügt `AWSManagedRulesACFProtectedRuleSet`.

13. Juni 2023

[Aktualisierung der Richtlinien zur Verhinderung von Kontoübernahmen \(ATP\) bei der AWS WAF Betrugsbekämpfung](#)

Sie können jetzt den Anmeldeendpunkt für die von ATP verwaltete Regelgruppe mithilfe eines regulären Ausdrucks angeben.

13. Juni 2023

[Neue Informationen für die CAPTCHA-API JavaScript](#)

In einem neuen Abschnitt wird beschrieben, wie Sie ein benutzerdefiniertes CAPTCHA-Puzzle lösen können, wenn Sie AWS WAF auf eine Anfrage mit einem CAPTCHA antworten.

13. Juni 2023

[Neue verwaltete ACFP-Regelgruppe](#)

Verwenden Sie die neue Regelgruppe `AWSManagedRulesACFPRuleSet`, um betrügerische Versuche zur Kontoerstellung zu erkennen und zu blockieren.

13. Juni 2023

[Einrichtung eines neuen Kontos bei der AWS WAF Betrugsbekämpfung und Betrugsprävention \(ACFP\)](#)

Mit der neuen verwalteten Regelgruppe zur AWS WAF Betrugsprävention bei der Kontoerstellung (ACFP) können Sie betrügerische Versuche zur Kontoerstellung erkennen und blockieren. `AWSManagedRulesACFPRuleSet` Bei geschützten CloudFront Distributionen können Sie ACFP auch verwenden, um neue Kontoerstellungsversuche von Kunden zu blockieren, die in letzter Zeit zu viele fehlgeschlagene Kontoerstellungsversuche eingereicht haben.

13. Juni 2023

[AWS WAF verwaltete Richtlinienänderungen](#)

`AWSWAFFullAccessPolicy`, `AWSWAFConsoleFullAccess`, und wurde aktualisiert `AWSWAFReadOnlyAccess`, `AWSWAFConsoleReadOnlyAccess` um die Zugriffseinstellungen für AWS App Runner Dienste zu korrigieren.

6. Juni 2023

Einschränkung für Firewall Manager Manager-Sicherheitsgruppenrichtlinien hinzugefügt	Wenn die gemeinsame Nutzung einer gemeinsam genutzten VPC später aufgehoben wird, löscht Firewall Manager die Replikat-Sicherheitsgruppen im zugehörigen Konto nicht.	02. Juni 2023
Neue Anforderungskomponente AWS WAF : Header order	Sie können jetzt einen Abgleich mit einer geordneten Liste der Namen der Header in der Anfrage durchführen.	30. Mai 2023
Aktualisierte AWS verwaltete Regeln für AWS WAF	Der Regelsatz für das Linux-Betriebssystem wurde aktualisiert.	22. Mai 2023
Die Organisation des AWS WAF Regelabschnitts wurde aktualisiert	Die Auflistungen der Regelerklärungen sind jetzt nach Auskunftstyp gruppiert.	16. Mai 2023
Das Thema wurde verschoben: IP-Adressen auflisten, deren Rate begrenzt ist	Das Thema zum Auflisten von IP-Adressen, für die eine ratenbasierte Regel gilt, befindet sich jetzt unter dem Thema Ratenbasierte Regeln.	16. Mai 2023

Erweiterte Optionen für ratenbasierte Regeln

Sie können jetzt die Rate von Webanfragen auf der Grundlage anderer Aggregationschlüssel als IP-Adressen begrenzen, und Sie können mithilfe von Schlüsselkombinationen aggregieren. Sie können auch ohne weitere Aggregation eine Ratenbegrenzung für alle Anfragen festlegen, die einer Scopedown-Anweisung entsprechen.

16. Mai 2023

Erhöhung des Firewall Manager Manager-Kontingents

Die Anzahl der Firewall Manager Manager-Richtlinien pro Organisation wurde von 20 auf 50 erhöht. Die maximale Anzahl primärer Sicherheitsgruppen pro Richtlinie wurde von eins auf drei erhöht. Die maximale Anzahl von WCUs wurde von einem weichen Kontingent auf ein festes Kontingent geändert.

5. Mai 2023

Die maximale Anzahl von WCUs pro Regelgruppe wurde erhöht

Sie können jetzt bis zu 5.000 Web-ACL-Kapazitätseinheiten (WCUs) pro Regelgruppe verwenden, ohne den Support um eine Erhöhung bitten zu müssen. Dieses neue Limit kann nicht erhöht werden.

1. Mai 2023

AWS WAF Amazon S3 S3-Log-Bucket-Speicherorte mit Präfixen	AWS WAF erlaubt jetzt Präfixe in Amazon S3 S3-Log-Bucket-Namen.	1. Mai 2023
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für die AWS WAF aktualisierte Regelgruppe des Kernregelsatzes (CRS).	28. April 2023
Unterstützung für AWS Verified Access-Instanzen wurde hinzugefügt zu AWS WAF	Sie können jetzt eine AWS WAF Web-ACL mit einer Verified Access-Instanz verknüpfen. Diese Änderung ist nur in der neuesten Version von AWS WAF und nicht in AWS WAF Classic verfügbar.	28. April 2023
Überarbeitetes Kapitel über die Arbeit mit mehreren Firewall Manager Manager-Administratoren	Sie können jetzt mehrere Firewall Manager Manager-Administratoren benennen, um die Firewall-Ressourcen Ihres Unternehmens zu erstellen und zu verwalten.	24. April 2023
AWS Firewall Manager verwaltetes Richtlinienupdate	Aktualisiert FMSServiceRolePolicy .	21. April 2023
Neue Integration von JavaScript Client-Anwendungen für CAPTCHA	Sie können jetzt die Platzierung und die Eigenschaften des CAPTCHA-Puzzles in Ihren Client-Anwendungen anpassen. JavaScript	20. April 2023

[Die Anwendungsintegration wurde in Intelligente Bedrohungsintegration umbenannt](#)

Wir haben die bestehende Funktionalität für die Integration von Client-Anwendungen in intelligente Bedrohungsintegrationen umbenannt, um die Unterscheidung zwischen dieser Funktion und der neuen CAPTCHA-Anwendungsintegration für zu erleichtern. JavaScript

20. April 2023

[Variable Preise für Web-ACL-WCUs über 1.500](#)

Die Verwendung von mehr als 1.500 Web-ACL-Kapazitätseinheiten (WCUs) in Ihrer Web-ACL verursacht zusätzliche Kosten, die automatisch angepasst werden, wenn Ihre Web-ACL-WCU-Nutzung zunimmt und sinkt. Das Web-ACL-Maximum liegt bei 5.000 WCUs.

11. April 2023

[Die maximale Anzahl von WCUs pro Web-ACL wurde erhöht](#)

Sie können jetzt bis zu 5.000 Web-ACL-Kapazitätseinheiten (WCUs) pro Web-ACL verwenden, ohne den Support um eine Erhöhung bitten zu müssen. Dieses neue Limit kann nicht erhöht werden.

11. April 2023

[Größenbeschränkungen bei der Körperinspektion für CloudFront Web-ACLs](#)

Für Web-ACLs, die CloudFront Amazon-Distributionen schützen, können Sie die Größenbeschränkung für die Körperinspektion in Ihrer Web-ACL-Konfiguration auf bis zu 64 KB erhöhen.

11. April 2023

[Erhöhung der Größe der Karosserieinspektion für CloudFront](#)

Die maximale Größenbeschränkung für AWS WAF Karosserieinspektionen für CloudFront Amazon-Distributionen wurde von 8 KB auf 64 KB erhöht. Die Standardgrößenbeschränkung für die Inspektion CloudFront beträgt 16 KB.

11. April 2023

[Neue Optionen AWS WAF für Richtlinienregeln in AWS Firewall Manager](#)

AWS Firewall Manager fügt Unterstützung für die Regelgruppen AWS WAF Fraud Control Account Takeover Prevention (ATP) und AWS WAF Bot Control AWS Managed Rules, Amazon S3 S3-Protokollierungsziele, Überschreibungen von Regelaktionen CAPTCHA und Challenge Regelaktionen sowie Token-Domainlisten hinzu.

7. April 2023

[Firewall Manager unterstützt Amazon S3 S3-Buckets als Protokollierungsziele für die AWS WAF Protokollierung](#)

Sie können jetzt Amazon S3 S3-Buckets als Protokollierungsziele in Ihren AWS WAF Richtlinien verwenden.

7. April 2023

AWS WAF verwaltete Richtlinienänderungen	AWSWAFFullAccessPolicy ,AWSWAFConsoleFullAccess , und wurde aktualisiertAWSWAFReadOnlyAccess , AWSWAFConsoleReadOnlyAccess um AWS App Runner Dienste zu den Ressourcentypen hinzuzufügen, mit denen Sie sich schützen können AWS WAF.	30. März 2023
Es wurde eine Warnung zur Verwendung von Tags in Sicherheitsgruppenrichtlinien hinzugefügt	Firewall Manager aktualisiert die Tags vorhandener Sicherheitsgruppen nicht und erstellt keine neuen Sicherheitsgruppen, wenn die Richtlinie Tags enthält, die mit der Tag-Richtlinie der Organisation in Konflikt stehen.	28. März 2023
Informationen zur Servicerolle werden aktualisiert	Die Verwendung einer Servicerolle mit Firewall Manager wurde aktualisiert.	08. März 2023
Informationen darüber, wie ratenbasierte Regeln die Ratenbegrenzung durchführen, wurden korrigiert	Bei ratenbasierten Regeln mit Angaben zum Geltungsbereich werden nur Anfragen mit Ratenbegrenzungen berücksichtigt, die mit der Angabe zum Geltungsbereich der Regel übereinstimmen. Wir gaben an, dass die Beschränkung für alle Anfragen für jede IP-Adresse mit begrenzter Rate gilt.	1. März 2023

Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für die AWS WAF aktualisierte Regelgruppe der PHP-Anwendung.	27. Februar 2023
Unterstützung für AWS App Runner bis hinzugefügt AWS WAF	Sie können jetzt eine AWS WAF Web-ACL mit einem AWS App Runner Dienst verknüpfen. Diese Änderung ist nur in der neuesten Version von AWS WAF und nicht in AWS WAF Classic verfügbar.	23. Februar 2023
Die IAM-Leitlinien für wurden aktualisiert AWS Firewall Manager	Aktualisierter Leitfaden, angepasst an die bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte IAM-Methoden .	16. Februar 2023
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für haben die Regelgruppe AWS WAF aktualisiert <code>AWSManagedRulesATPRuleSet</code> , um die Überprüfung von Login-Antworten in Web-ACLs zum Schutz von CloudFront Amazon-Distributionen hinzuzufügen.	15. Februar 2023
AWS WAF Überprüfung von Antworten auf Login-Antworten zur Verhinderung von Kontoübernahmen (ATP) bei der Betrugsbekämpfung	Für geschützte CloudFront Distributionen können Sie jetzt ATP verwenden, um neue Anmeldeversuche von Kunden zu blockieren, die in letzter Zeit zu viele fehlgeschlagene Anmeldeversuche eingereicht haben.	15. Februar 2023

Aktualisierte AWS verwaltete Regeln für AWS WAF	Der Kernregelsatz wurde aktualisiert.	25. Januar 2023
Bewährte Methoden für intelligente Bedrohungsabwehr	Es wurde ein Abschnitt mit bewährten Methoden für die Implementierung von Bot Control, ATP und anderen intelligenten Funktionen zur Bedrohungsabwehr hinzugefügt.	22. Januar 2023
Wie untersucht man HTTP/2-Pseudo-Header	Es wurde ein Abschnitt hinzugefügt, der HTTP/2-Pseudo-Header ihren entsprechenden Webanforderungskomponenten zuordnet.	20. Januar 2023
Die IAM-Leitlinien für Classic wurden aktualisiert AWS WAF	Aktualisierter Leitfaden, angepasst an die bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte IAM-Methoden .	3. Januar 2023
Die IAM-Leitlinien für wurden aktualisiert AWS WAF	Aktualisierter Leitfaden, angepasst an die bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte IAM-Methoden .	3. Januar 2023
Die IAM-Leitlinien für wurden aktualisiert AWS Shield	Aktualisierter Leitfaden, angepasst an die bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte IAM-Methoden .	3. Januar 2023

Aktualisierung der Amazon Route 53 Resolver DNS-Firewall-Richtlinien	Es wurden Informationen zum Löschen von Amazon Route 53 Resolver DNS-Firewall-Regelgruppen hinzugefügt.	29. Dezember 2022
Aktualisierte AWS verwaltete Regeln für AWS WAF	Der Regelsatz für das Linux-Betriebssystem wurde aktualisiert.	15. Dezember 2022
Aktualisierte AWS verwaltete Regeln für AWS WAF	Der Kernregelsatz wurde aktualisiert.	5. Dezember 2022
Firewall Manager bietet Unterstützung für Fortigate Cloud Native Firewall (CNF) as a Service-Richtlinien	Firewall Manager unterstützt jetzt die Fortigate CNF-Richtlinien.	2. Dezember 2022
Die AWS Config Anforderung für DNS-Firewall-Richtlinien wurde entfernt	Für DNS-Firewall-Richtlinien müssen Sie Config jetzt nur noch für den Ressourcentyp EC2 VPC aktivieren.	17. November 2022
AWS Firewall Manager verwaltetes Richtlinienupdate	Aktualisiert FMSServiceRolePolicy .	15. November 2022
Erweiterung der Sprachoptionen für das AWS WAF CAPTCHA-Puzzle	Das CAPTCHA-Puzzle bietet seine schriftlichen Anweisungen jetzt in mehreren Sprachen. Die Anweisungen in jedem Audiopuzzle sind weiterhin nur in englischer Sprache verfügbar.	11. November 2022
Neue Firewall Manager Manager-Kontingente für Ressourcensätze	Neue Kontingente für Ressourcensätze hinzugefügt.	08. November 2022

Unterstützung für Ressourcensätze hinzugefügt	Sie können Ressourcensätze erstellen, um Ressourcen zu gruppieren, die in einer Firewall Manager Richtlinie verwaltet werden sollen.	08. November 2022
Unterstützung für den Import von Firewalls aus der Network Firewall hinzufügen	Sie können jetzt vorhandene Firewalls in Netzwerk-Firewall-Richtlinien mithilfe von Ressourcensätzen importieren und verwalten.	08. November 2022
AWS Firewall Manager verwaltetes Richtlinien-Update	Aktualisiert AWSFMAAdminReadOnlyAccess .	02. November 2022
Geo Match Statement fügt Anfragen jetzt Labels für Länder und Regionen hinzu	Sie können jetzt den Ursprung geografischer Anfragen auf regionaler Ebene verwalten , indem Sie den Geoabgleich mit dem Label-Abgleich kombinieren.	31. Oktober 2022
Der Bereich auf oberster Ebene wurde umbenannt: Verwaltete Schutzmaßnahmen	Der Abschnitt trägt jetzt den Namen AWS WAF Intelligent Threat Mitigation, was mit unseren Marketingseiten übereinstimmt.	27. Oktober 2022
Neue gezielte Schutzstufe in der verwalteten Regelgruppe Bot Control	Die verwaltete Regelgruppe von Bot Control bietet jetzt zusätzliche, gezielte Regeln für die Erkennung und Abwehr ausgeklügelter Bots. Diese Schutzstufe ist gegen zusätzliche Gebühren erhältlich.	27. Oktober 2022

[Neuer Abschnitt über AWS WAF Tokens](#)

Erfahren Sie, wie Tokens zur intelligenten Abwehr von Bedrohungen AWS WAF verwendet werden.

27. Oktober 2022

[Wichtiger Hinweis zur Aktualisierung der Firewall Manager-Netzwerk-Firewall-Richtlinien hinzugefügt](#)

Wenn Sie eine Firewall Manager-Manager-Richtlinie aktualisieren, werden alle Netzwerk-Firewall-Richtlinien, die durch die Richtlinie erstellt wurden, mit der Netzwerk-Firewall-Richtlinienkonfiguration der Firewall Manager-Richtlinie aktualisiert.

27. Oktober 2022

[Überschreibungen von Aktionen in Regelgruppen](#)

Sie können jetzt die Aktionen der Regeln in einer Regelgruppe mit jeder beliebigen Regelaktionseinstellung überschreiben. Wie bei der vorherigen Count-Aktionsüberschreibung können Sie Ihre Überschreibungen auf alle Regeln in einer Regelgruppe und auf einzelne Regeln anwenden.

27. Oktober 2022

[AWS WAF neue Option für Challenge-Regelaktionen](#)

Sie können Regeln so konfigurieren, dass sie verwenden `Challenge`, um zu überprüfen, ob Anfragen von Browsern gesendet werden.

27. Oktober 2022

AWS WAF ermöglicht die gemeinsame Nutzung von Token zwischen mehreren geschützten Anwendungen	Sie können die Verwendung von Token für mehrere geschützte Anwendungen aktivieren, indem Sie eine Token-Domainliste für Ihre Web-ACL konfigurieren.	27. Oktober 2022
Bei der Angabe aller Header wird nicht zwischen Groß- und Kleinschreibung unterschieden	Die Spezifikation für alle Header wurde dahingehend geändert, dass Groß- und Kleinschreibung nicht berücksichtigt wird. Dies entspricht dem Verhalten einzelner Header.	26. Oktober 2022
AWS Firewall Manager Änderungen der Richtlinien	Die Richtlinienliste für die manuelle Gewährung des vollen Zugriffs auf AWS Firewall Manager Ressourcen wurde aktualisiert.	21. Oktober 2022
AWS Firewall Manager verwaltete Richtlinienänderungen	Korrekturen an <code>AWSFMAdminFullAccess</code> .	21. Oktober 2022
Aktualisierte AWS verwaltete Regeln für AWS WAF	Die Regelgruppe für bekannte fehlerhafte Eingaben wurde aktualisiert.	20. Oktober 2022
Aktualisierte AWS verwaltete Regeln für AWS WAF	Die Regelgruppe für bekannte fehlerhafte Eingaben wurde aktualisiert.	5. Oktober 2022
Aktualisierung der SDK-Spezifikation AWS WAF für Mobilgeräte	Der Standardwert für <code>tokenRefreshDelaySec</code> von 600 (10 Minuten) auf 300 (5 Minuten) gesenkt.	30. September 2022

[Aktualisierte AWS verwaltete Regeln für AWS WAF](#)

Die in dieser Dokumentation angegebenen Labelnamen für die folgenden Regelgruppen wurden korrigiert: POSIX-Betriebssystem, PHP-Anwendung, WordPress Anwendung.

19. September 2022

[Neue Option AWS WAF für Richtlinienregeln in AWS Firewall Manager](#)

AWS Firewall Manager unterstützt jetzt benutzerdefinierte Webanfragen und Antworten für Standard-Webaktionen in AWS WAF Richtlinien.

09. September 2022

[Aktualisierte AWS verwaltete Regeln für AWS WAF](#)

AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: IP-Reputation.

30. August 2022

[AWS WAF verwaltete Richtlinienänderungen](#)

Aktualisiert AWS WAF FullAccessPolicy, AWS WAF Console FullAccess, AWS WAF ReadOnlyAccess, und AWS WAF Console ReadOnlyAccess um Amazon Cognito Cognito-Benutzerpools zu den Ressourcentypen hinzuzufügen, mit AWS WAF denen Sie sich schützen können.

25. August 2022

[AWS WAF Verhinderung von Kontoübernahmen \(ATP\) bei der Betrugsbekämpfung](#)

Sie können jetzt die ATP-Funktion (AWS WAF Fraud Control Account Takeover Prevention) bei CloudFront Amazon-Distributionen verwenden.

24. August 2022

[Aktualisierte AWS verwaltete Regeln für AWS WAF](#)

AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: Bekannte fehlerhafte Eingaben.

22. August 2022

[Aktualisierte AWS verwaltete Regeln für AWS WAF](#)

AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen:AWSManagedRulesATPRuleSet .

11. August 2022

[Unterstützung für Amazon Cognito Cognito-Benutzerpools hinzugefügt zu AWS WAF](#)

Sie können jetzt eine AWS WAF Web-ACL mit einem Amazon Cognito Cognito-Benutzerpool verknüpfen. Diese Änderung ist nur in der neuesten Version von AWS WAF und nicht in AWS WAF Classic verfügbar.

11. August 2022

Es wurde ein Abschnitt über Bereitstellungen für versionierte Regelgruppen mit AWS verwalteten Regeln hinzugefügt	Es wurde ein neuer Abschnitt hinzugefügt, der Bereitstellungen für versionierte AWS Regelgruppen mit verwalteten Regeln dokumentiert. Dieser Abschnitt enthält Informationen darüber, wie Standardversionen bei Release-Candidate-Bereitstellungen benannt werden.	29. Juli 2022
Aktualisierte Anforderungen für die Konfiguration der Protokollierung für Netzwerk-Firewall-Richtlinien	Es wurden Anforderungen für Netzwerk-Firewall-Richtlinien hinzugefügt, die einen verschlüsselten Amazon S3 S3-Bucket als Protokollziel verwenden.	26. Juli 2022
Option zur Sensitivitätsstufe für SQLi-Regelanweisungen	Sie können jetzt die Sensitivität Ihrer SQL-Injection-Regelanweisungen erhöhen. Dies ändert nichts am Verhalten vorhandener Anweisungen, deren Sensitivitätsstufe standardmäßig istLOW.	15. Juli 2022
Option zur Konfiguration der Netzwerk-Firewall-Richtlinie hinzugefügt	Firewall Manager unterstützt jetzt statusbehaftete Bewertungsreihenfolge und Standardaktionen in den Firewall-Richtlinienkonfigurationen der Network Firewall.	14. Juli 2022
Aktualisierungen der Einstellungen der Sicherheitsgruppen richtlinienregeln von Firewall Manager	Firewall Manager unterstützt jetzt die Tag-Verteilung von primären Sicherheitsgruppen an Replikatsicherheitsgruppen.	7. Juli 2022

Aktualisierungen des Handbuchs AWS Shield	Die Informationen im Shield-Handbuch wurden erweitert , um zu beschreiben, wie Shield die Ereignisbegrenzung durchführt.	24. Juni 2022
Die Anleitung zum Testen und Optimieren von AWS WAF Schutzmaßnahmen wurde aktualisiert	Die allgemeinen Leitlinien zum Testen und Optimieren AWS WAF wurden aktualisiert und sind jetzt ein Top-Thema.	20. Juni 2022
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: Core Rule Set (CRS).	9. Juni 2022
Neue Firewall Manager verwirrte stellvertretende Führung	Es wurde eine Anleitung hinzugefügt, wie das Problem mit dem verwirrten Stellvertreter für Firewall Manager verhindert werden kann.	1. Juni 2022
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: Core Rule Set (CRS).	24. Mai 2022
Neue AWS WAF Anforderungskomponenten: Headers und Cookies	Sie können die Cookies jetzt in einer Webanforderung einsehen und alle Header in einer Webanforderung zusätzlich zu einem einzigen Header überprüfen.	29. April 2022

[AWS WAF Umgang mit
übergroßen Textteilen,
Headern und Cookie-Anforderungskomponenten](#)

Sie können jetzt innerhalb Ihrer Regeln, die diese AWS WAF Komponenten überprüfen, angeben, wie mit übergroßen Anforderungstexten, Headern und Cookies umgegangen werden soll. Regeln, die Sie bereits erstellt haben und die diese Komponenten untersuchen, weisen ein Verhalten auf, das der neuen Continue Option für die Behandlung übergroßer Komponenten entspricht.

29. April 2022

[AWS WAF Änderungen der
Amazon S3 S3-Protokollrichtlinie](#)

Die Richtlinie für Protokollberechtigungen und das Beispiel von Amazon S3 wurden aktualisiert.

12. April 2022

[Option zur automatischen
DDoS-Abwehr auf Anwendungsebene jetzt AWS Shield
Advanced für Application Load
Balancer verfügbar](#)

Shield Advanced unterstützt jetzt die automatische DDoS-Abwehr auf Anwendungsebene für Application Load Balancer und ist somit für alle Schutzmaßnahmen auf Anwendungsebene verfügbar. Sie können Shield Advanced so konfigurieren, dass die Webanfragen, die Teil eines DDoS-Angriffs auf Anwendungsebene auf eine geschützte Ressource sind, automatisch gezählt oder blockiert werden.

8. April 2022

Es wurde ein Indikator für die aktuelle Standardversionseinstellung für verwaltete Regelgruppen hinzugefügt	In Versionslisten für verwaltete Regelgruppen wird jetzt angegeben, welche Version der aktuelle Standard ist.	8. April 2022
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: AWS WAF Bot Control.	6. April 2022
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: Bekannte fehlerhafte Eingaben.	31. März 2022
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: Bekannte fehlerhafte Eingaben.	30. März 2022
Firewall Manager bietet Unterstützung für die Palo Alto Networks Cloud Next Generation Firewall (NGFW)	Firewall Manager unterstützt jetzt die Palo Alto Networks Cloud Next Generation Firewall (NGFW).	30. März 2022
Fügen Sie Unterstützung für Palo Alto Networks Cloud NGFW hinzu zu AWS Firewall Manager	AWS Firewall Manager unterstützt jetzt die Richtlinien der Palo Alto Networks Cloud Next Generation Firewall (NGFW).	30. März 2022

Aktualisierungen des Leitfadens AWS Shield	Die Informationen im Shield-Leitfaden wurden erweitert , um zu beschreiben, wie Shield die Ereigniserkennung durchführt, und um Beispiele für DDoS-resistente Architekturen bereitzustellen.	16. März 2022
Aktualisierungen des Leitfadens AWS Shield	Die Informationen im Shield-Leitfaden wurden erweitert und die Organisation verschiedener Abschnitte verbessert. Die wichtigsten Änderungen betreffen die folgenden Abschnitte des Shield-Leitfadens: Unterstützung des Shield Response Team (SRT), Ressourcenschutz in AWS Shield Advanced und Sichtbarkeit von DDoS-Ereignissen.	28. Februar 2022
Firewall Manager unterstützt jetzt das zentralisierte Bereitstellungsmodell von Network Firewall	Es wurde ein neues Verfahren hinzugefügt, das erklärt, wie Richtlinien konfiguriert werden, die verteilte und zentralisierte Bereitstellungsmodelle verwenden.	24. Februar 2022

[Firewall Manager bietet Unterstützung für das AWS Network Firewall zentralisierte Bereitstellungsmodell](#)

Sie können Ihre AWS Network Firewall Richtlinien jetzt so konfigurieren, dass sie entweder das verteilte oder das zentralisierte Bereitstellungsmodell verwenden. Mit dem verteilten Bereitstellungsmodell erstellt und verwaltet Firewall Manager Firewall-Endpunkte in jeder VPC, die sich innerhalb des Richtlinienbereichs befinden. Mit dem zentralisierten Bereitstellungsmodell erstellt und verwaltet Firewall Manager Firewall-Endpunkte in einer einzigen Inspektions-VPC.

24. Februar 2022

[Fügen Sie Unterstützung für die AWS WAF verwaltete Versionierung von Regelgruppen hinzu AWS Firewall Manager](#)

AWS Firewall Manager unterstützt jetzt die AWS WAF verwaltete Versionierung von Regelgruppen in Firewall Manager AWS WAF Manager-Richtlinien.

18. Februar 2022

[AWS Firewall Manager verwaltete Richtlinienänderung](#)

Update auf `FMSServiceRolePolicy`

16. Februar 2022

[Aktualisierte AWS verwaltete Regeln für AWS WAF](#)

AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: IP-Reputationslisten.

15. Februar 2022

[Aktualisierte AWS verwaltete Regeln für AWS WAF](#)

AWS Verwaltete Regeln für AWS WAF haben die Regelgruppe zur Verhinderung von Kontoübernahmen (AWS WAF Fraud Control Account Takeover Prevention, ATP) hinzugefügt `AWSManagedRulesATPRuleSet` .

11. Februar 2022

[Änderungen an der Organisation des AWS WAF Leitfadens](#)

Auf oberster Ebene wurde ein neuer Abschnitt zu verwalteten Schutzvorkehrungen hinzugefügt. Der CAPTCHA-Abschnitt wurde vom Abschnitt zu den Regeln in den neuen Abschnitt zu verwalteten Schutzvorkehrungen verschoben. Der Abschnitt zu Labels wurde vom Abschnitt zu den Regeln in einen eigenen Abschnitt auf oberster Ebene verschoben.

11. Februar 2022

[AWS WAF Integrationen von Client-Anwendungen](#)

Verwenden Sie die APIs AWS WAF JavaScript und die mobilen Client-APIs, um Ihre Client-Anwendungen in die Regelgruppen AWS Managed Rules zur intelligenten Bedrohungsabwehr zu integrieren und so die Erkennung zu verbessern.

11. Februar 2022

AWS WAF Verhinderung von Kontoübernahmen (ATP) bei der Betrugsbekämpfung	Mit der neuen verwalteten Regelgruppe zur Verhinderung von Kontoübernahmen (AWS WAF Fraud Control Account Takeover Prevention, ATP) können Sie Versuche zur Kontoübernahme erkennen und blockierenAWSManagedRulesATPRuleSet .	11. Februar 2022
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: Bekannte fehlerhafte Eingaben.	28. Januar 2022
AWS WAF verwaltete Richtlinienänderungen	AWSWAFFullAccessPolicy und AWSWAFConsoleFullAccess wurden aktualisiert, um die Berechtigungen für die Protokollierung zu korrigieren.	11. Januar 2022
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: Kernregelsatz (CRS), SQLi-Datenbank.	10. Januar 2022
Firewall Manager unterstützt die automatische DDoS-Abwehr von Shield Advanced auf Anwendungsebene	Die erweiterten Richtlinien von Firewall Manager Shield für CloudFront Amazon-Ressourcen bieten jetzt Unterstützung für die automatische DDoS-Abwehr auf Anwendungsebene.	7. Januar 2022

AWS Firewall Manager verwaltete Richtlinienänderung	Update auf <code>FMSServiceRolePolicy</code> .	7. Januar 2022
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: Bekannte fehlerhafte Eingaben.	17. Dezember 2021
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: Bekannte fehlerhafte Eingaben.	11. Dezember 2021
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: Bekannte fehlerhafte Eingaben.	10. Dezember 2021
Neue AWS Shield Advanced serviceverknüpfte Rolle	Es wurde hinzugefügt <code>AWSServiceRoleForAWSShield</code> , um die automatische Funktion zur DDoS-Abwehr auf Anwendungsebene zu unterstützen.	1. Dezember 2021
Neue verwaltete Richtlinie AWS Shield	<code>AWSShieldServiceRolePolicy</code> Zur Unterstützung der automatischen DDoS-Abwehrfunktion auf Anwendungsebene hinzugefügt.	1. Dezember 2021

Die Option zur automatischen DDoS-Abwehr auf Anwendungsebene ist jetzt verfügbar mit für AWS Shield Advanced CloudFront	Shield Advanced unterstützt jetzt automatische DDoS-Abwehr auf Anwendungsebene für CloudFront Amazon-Distributionen. Sie können Shield Advanced so konfigurieren, dass die Webanfragen, die Teil eines DDoS-Angriffs auf Anwendungsebene auf eine CloudFront Distribution sind, automatisch gezählt oder blockiert werden.	1. Dezember 2021
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: Kernregelsatz (CRS), Windows-Betriebssystem, Linux-Betriebssystem und IP-Reputationslisten.	23. November 2021
AWS Firewall Manager verwaltete Richtlinienänderung	Update auf <code>FMSServiceRolePolicy</code> .	18. November 2021
Erweiterte Protokollierungsoptionen für AWS WAF	Sie können jetzt Web-ACL-Verkehr in einer Amazon CloudWatch Logs-Protokollgruppe oder einem Amazon Simple Storage Service (Amazon S3) -Bucket protokollieren. Diese Optionen ergänzen die bestehende Option, sich bei einer Amazon Data Firehose anzumelden.	15. November 2021

AWS WAF verwaltete Richtlinienänderungen	AWSWAFFullAccessPolicy und AWSWAFConsoleFullAccess wurden aktualisiert, um zusätzlich Protokollierungsziele zu unterstützen.	15. November 2021
AWS WAF neue Option für CAPTCHA Regelaktionen	Sie können Regeln so konfigurieren, dass ein CAPTCHA für Webanfragen ausgeführt und bei Bedarf ein CAPTCHA-Problem an den Client gesendet wird.	8. November 2021
Aktualisierte verwaltete Regeln für AWSAWS WAF	AWS Verwaltete Regeln für die AWS WAF aktualisierte Regelgruppe des Kernregelsatzes (CRS).	27. Oktober 2021
Aktualisierte AWS verwaltete Regeln für AWS WAF	Alle Regelgruppen für AWS verwaltete Regeln unterstützen jetzt die Kennzeichnung. Die Regelbeschreibungen enthalten die Kennzeichnungsspezifikationen.	25. Oktober 2021
Firewall Manager unterstützt die Netzwerk-Firewall-Protokollfilterung	AWS Firewall Manager unterstützt jetzt die Protokollfilterung für Netzwerk-Firewall-Richtlinien.	4. Oktober 2021
AWS Firewall Manager verwaltete Richtlinienänderung	Update aufFMSServiceRolePolicy .	29. September 2021
Regex-Match-Anweisung hinzugefügt	Sie können Webanforderungen jetzt mit einem einzelnen regulären Ausdruck abgleichen.	22. September 2021

Ratenbasierte Regeln innerhalb von Regelgruppen AWS WAF	Sie können jetzt ratenbasierte Regeln innerhalb von Regelgruppen definieren. AWS WAF In AWS Firewall Manager, diese Funktion wird für AWS WAF Richtlinien vollständig unterstützt.	13. September 2021
Firewall Manager unterstützt die AWS WAF Protokollfilterung	AWS Firewall Manager unterstützt jetzt die Protokollfilterung für AWS WAF Richtlinien.	31. August 2021
Automatisches Entfernen von out-of-scope Ressourcenschutzmaßnahmen in AWS Firewall Manager	AWS Firewall Manager ermöglicht es Ihnen, automatisch Schutzmaßnahmen für Ressourcen zu entfernen, die nicht in den Geltungsbereich der Richtlinie fallen.	25. August 2021
AWS Firewall Manager verwaltete Richtlinienänderung	Update auf <code>FMSServiceRolePolicy</code> .	12. August 2021
Versionierung zu verwalteten Regelgruppen hinzugefügt	Anbieter von verwalteten Regelgruppen können ihre Regelgruppen jetzt versionieren.	9. August 2021
Ändern Sie die AWS Firewall Manager Administratoranforderungen	Sie können das Verwaltungskonto der Organisation als Firewall Manager Administratorkonto verwenden. Dies war nicht erlaubt worden.	2. August 2021

Erhöhung des Firewall Manager Manager-Kontingents	Die Anzahl der Amazon VPC-Instances, die Sie im Rahmen einer Firewall Manager Manager-Richtlinie haben können, wurde von 10 auf 100 erhöht.	28. Juli 2021
AWS Firewall Manager Unterstützung für die Überwachung von AWS Network Firewall Routing-Tabellen	AWS Firewall Manager unterstützt jetzt die Überwachung von Routing-Tabellen und gibt Sicherheitsadministratoren Empfehlungen zur Behebung von AWS Network Firewall Richtlinien mit falsch konfigurierten Routen.	8. Juli 2021
AWS WAF zusätzliche Optionen für die Texttransformation	Erweiterte Optionen für Texttransformationen, die Sie auf Webanforderungskomponenten anwenden können, bevor Sie sie überprüfen.	24. Juni 2021
Geänderte Benennung für Firewall Manager AWS WAF Manager-Richtlinienressourcen	Die Benennung der Web-ACLs, Regelgruppen und Protokollierung, die Firewall Manager für Ihre AWS WAF Richtlinien verwaltet, hat sich geändert.	26. Mai 2021
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für AWS WAF zusätzliche Unterstützung für die Kennzeichnung von IP-Reputationslisten und entfernte Suffixe auf Regelnamen für die Amazon-IP-Reputationsliste.	4. Mai 2021

[Unterstützung für Delegated Administrator AWS Organizations hinzufügen](#)

Wenn Sie das AWS Firewall Manager Administratorkonto einrichten, bestimmt Firewall Manager das Konto jetzt als AWS Organizations delegierten Administrator für Firewall Manager. Mit dieser Änderung müssen Sie bei der Einrichtung des Firewall Manager-Administratorkontos ein anderes Mitgliedskonto als das Verwaltungskonto der Organisation angeben. Diese Änderung hat keine Auswirkungen auf Ihre vorhandenen Einstellungen.

30. April 2021

[Aktualisierte AWS verwaltete Regeln für AWS WAF](#)

AWS Verwaltete Regeln für AWS WAF haben die Regelgruppe AWS WAF Bot Control hinzugefügt.

01. April 2021

[Legen Sie einzelne Regelaktionen Count in einer Regelgruppe fest](#)

Sie können jetzt die einzelnen Regelaktionen in einer Regelgruppe auf festlegen Count. Die Informationen für die vorhandene Überschreibung auf Regelgruppenebene wurden korrigiert.

01. April 2021

[Erläuterung des Geltungsbereichs für verwaltete Regelgruppen](#)

Sie können jetzt eine Eingrenzungsanweisung mit verwalteten Regelgruppen auf die gleiche Weise wie mit einer ratenbasierten Anweisung verwenden.

01. April 2021

Filterung von Protokollen	Sie können jetzt den Web-ACL-Datenverkehr, den Sie protokollieren, auf der Grundlage von Regelaktion und Bezeichnung filtern.	01. April 2021
AWS WAF Labels auf Webanfragen	Sie können Regeln konfigurieren, um übereinstimmenden Webanforderungen Bezeichnungen hinzuzufügen und Bezeichnungen abzugleichen, die durch andere Regeln hinzugefügt werden.	01. April 2021
AWS WAF Bot-Steuerung	Sie können den Bot-Verkehr mit der neuen AWS WAF Bot Control-Funktion überwachen und kontrollieren. Sie kombiniert die von Bot Control verwaltete Regelgruppe mit der Kennzeichnung von Webanfragen, Scopedown-Anweisungen und Protokollfilterung.	01. April 2021
Firewall Manager unterstützt Amazon Route 53 Resolver DNS-Firewall-Richtlinien	AWS Firewall Manager unterstützt die zentrale Verwaltung der Filterung des ausgehenden DNS-Datenverkehrs mit Amazon Route 53 Resolver DNS Firewall für Ihre VPCs.	31. März 2021

Benutzerdefinierte Bearbeitung von Anfragen und Antworten	Sie können benutzerdefinierte Header für Webanfragen hinzufügen, die AWS WAF nicht blockiert werden, und Sie können benutzerdefinierte Antworten für AWS WAF blockierte Webanfragen senden. Dies ist für die Einstellungen für Web-ACL-Standardaktionen und Regelaktionen verfügbar.	29. März 2021
AWS Firewall Manager verwaltete Richtlinienänderung	Update auf <code>FMSServiceRolePolicy</code> .	17. März 2021
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für AWS WAF aktualisierte die folgenden Regelgruppen: Kernregelsatz (CRS), Administratorschutz, bekannte fehlerhafte Eingaben und Linux-Betriebssystem.	3. März 2021
AWS Shield verwaltete Nachverfolgung von Richtlinienänderungen	Shield begann, Änderungen für seine AWS verwalteten Richtlinien zu verfolgen.	3. März 2021
AWS Firewall Manager verwaltete die Nachverfolgung von Richtlinienänderungen	Firewall Manager begann, Änderungen für seine AWS verwalteten Richtlinien zu verfolgen.	2. März 2021
AWS WAF verwaltete Nachverfolgung von Richtlinienänderungen	AWS WAF hat begonnen, Änderungen an den AWS verwalteten Richtlinien zu verfolgen.	1. März 2021

Untersuchen Sie den Hauptteil einer Webanfrage als geparstes JSON	Es wurde die Option hinzugefügt, den Webanforderungstext als analysierten und gefilterten JSON-Code zu untersuchen. Dies gilt zusätzlich zu der vorhandenen Option, den Webanforderungstext als Klartext zu untersuchen.	12. Februar 2021
Firewall Manager unterstützt AWS Network Firewall Richtlinien	AWS Firewall Manager unterstützt die zentrale Verwaltung der Filterung des AWS Network Firewall Netzwerkverkehrs für Ihre VPCs.	17. November 2020
Unterstützung für AWS Shield Advanced Schutzgruppen hinzufügen	Sie können Ihre geschützten Ressourcen jetzt in logische Gruppen gruppieren und deren Schutzmaßnahmen gemeinsam verwalten.	13. November 2020
Unterstützung für AWS AppSync hinzugefügt AWS WAF	Sie können Ihrer AWS AppSync GraphQL-API jetzt eine AWS WAF Web-ACL zuordnen. Diese Änderung ist nur in der neuesten Version von AWS WAF und nicht in AWS WAF Classic verfügbar.	1. Oktober 2020
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für den AWS WAF aktualisierten Regelsatz des Windows-Betriebssystems.	23. September 2020

Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für AWS WAF aktualisierte Regelsätze, PHP-Anwendung und POSIX-Betriebssystem.	16. September 2020
Aktualisierte Konsole AWS Shield	AWS Shield bietet eine neue Konsolenoption mit einer verbesserten Benutzere rfahrung. Die Konsolena nleitung in der Dokumenta tion bezieht sich auf die neue Konsole.	1. September 2020
Firewall Manager Manager-Updates für allgemeine Sicherheitsgruppenrichtlinien	AWS Firewall Manager Allgemeine Sicherhei tsgruppenrichtlinien unterstüt zen jetzt die Ressourcentypen Application Load Balancers und Classic Load Balancers über die Konsolenimplementi erung. Die neuen Optionen sind in den Einstellungen für den Geltungsbereich der gemeinsamen Richtlinie verfügbar.	11. August 2020
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für den AWS WAF aktualisierten Kernregelsatz.	7. August 2020
Firewall Manager unterstüt zt die AWS WAF Protokoll ierungskonfiguration	AWS Firewall Manager unterstützt jetzt die zentralis ierte Protokollierungsko nfiguration für AWS WAF Richtlinien.	30. Juli 2020

[Geben Sie den Standort der IP-Adresse in der Webanfrage an](#)

Es wurde die Option hinzugefügt, IP-Adressen aus einem von Ihnen angegebenen HTTP-Header zu verwenden, anstatt den Ursprung der Webanforderung zu verwenden. Der alternative Header ist üblicherweise X-Forwarded-For (XFF), aber Sie können einen beliebigen Header-Namen angeben. Sie können diese Option für IP-Set-Abgleich, den Geoabgleich und die ratenbasierte Regelanzahlaggregation verwenden.

9. Juli 2020

[Firewall Manager Manager-Updates für Sicherheitsgruppenrichtlinien zur Inhaltsüberwachung](#)

AWS Firewall Manager hat die Funktionalität für Inhaltsaudit-Sicherheitsgruppenrichtlinien erweitert, einschließlich einer Option für verwaltete Regeln, die verwaltete Anwendungs- und Protokolllisten sowie Details zu Ressourcenverstößen verwendet.

7. Juli 2020

[Von Firewall Manager verwaltete Listen](#)

AWS Firewall Manager unterstützt jetzt verwaltete Anwendungs- und Protokolllisten. Firewall Manager verwaltet einige Listen und Sie können Ihre eigenen erstellen und verwalten.

7. Juli 2020

<u>Firewall Manager unterstützt gemeinsam genutzte VPCs in gemeinsamen Sicherheitsgruppenrichtlinien</u>	AWS Firewall Manager unterstützt jetzt die Verwendung gemeinsamer Sicherheitsgruppenrichtlinien in gemeinsam genutzten VPCs. Dies ist zusätzlich zur Verwendung in VPCs im Besitz von Konten im Geltungsbereich möglich.	26. Mai 2020
<u>Aktualisierte AWS verwaltete Regeln für AWS WAF</u>	Dokumentation für jede Regel in den AWS verwalteten Regeln für hinzugefügt AWS WAF.	20. Mai 2020
<u>Aktualisierte AWS verwaltete Regeln für AWS WAF</u>	AWS Verwaltete Regeln für die AWS WAF aktualisierte Regelgruppe des Linux-Betriebssystems.	19. Mai 2020
<u>Unterstützung für die Migration von AWS WAF Classic-Ressourcen auf AWS WAF (v2) hinzugefügt</u>	Sie können jetzt die Konsole oder API verwenden, um Ihre AWS WAF Classic-Ressourcen für die Migration auf die neueste Version von AWS WAF zu exportieren.	27. April 2020

[Fügen Sie Unterstützung für AWS Organizations Organisationseinheiten im Geltungsbereich der Richtlinie hinzu](#)

AWS Firewall Manager unterstützt jetzt die Verwendung von AWS Organizations Organisationseinheiten (OUs) zur Festlegung des Richtlinienbereichs. Sie können Organisationseinheiten (OUs) verwenden, um Konten in den Bereich einzuschließen oder davon auszuschließen, zusätzlich zum Ein- oder Ausschließen bestimmter Konten. Die Angabe einer OU ist identisch mit der Angabe aller Konten in der OU und ihren untergeordneten OUs, einschließlich aller untergeordneten OUs und Konten, die zu einem späteren Zeitpunkt hinzugefügt werden.

6, 2020. April 2020

[Unterstützung für AWS WAF \(v2\) hinzugefügt zu AWS Firewall Manager](#)

AWS Firewall Manager unterstützt jetzt zusätzlich zur AWS WAF Vorgängerversion die neueste Version von AWS WAF Classic.

31. März 2020

Aktualisierung der AWS Firewall Manager allgemeinen Sicherheitsgruppenrichtlinien	AWS Firewall Manager Die gemeinsame Sicherheitsgruppenrichtlinie bietet jetzt die Option, die Richtlinie auf alle elastischen Netzwerkschnittstellen in Ihren Amazon EC2 EC2-Instances anzuwenden, die in den Geltungsbereich fallen. Sie können die Richtlinie aber auch weiterhin nur auf die standardmäßige Elastic Network-Schnittstelle anwenden.	11. März 2020
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für eine AWS WAF hinzugefügte <code>AWSManagedRulesAnonymousIpList</code> Regelgruppe.	6. März 2020
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Verwaltete Regeln für AWS WAF aktualisierte WordPress Anwendungs- und <code>AWSManagedRulesCommonRuleSet</code> Regelgruppen.	3. März 2020
Amazon Route 53 Health Check wurde zu den AWS Shield Advanced Schutzoptionen hinzugefügt	Shield Advanced unterstützt jetzt die Verwendung von Amazon Route 53-Zuordnungen zur Gesundheitsprüfung, um die Genauigkeit der Erkennung und Abwehr von Bedrohungen zu verbessern.	14. Februar 2020

Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Managed Rules for AWS WAF hat die SQL-Datenbank-Regelgruppe um die Überprüfung des Nachrichten-URI erweitert.	23. Januar 2020
Firewall Manager: Neue Option für die Audit-Richtlinie zur Nutzung von Sicherheitsgruppen	Firewall Manager bietet eine neue Option für Überwachungsrichtlinien für die Nutzung von Sicherheitsgruppen. Sie können jetzt eine Mindestanzahl von Minuten festlegen, die eine Sicherheitsgruppe unbenutzt bleiben muss, bevor sie als nicht konform angesehen wird. Standardmäßig ist diese Einstellung auf null Minuten festgelegt.	14. Januar 2020
Firewall Manager, neue Option für AWS WAF Richtlinien	Firewall Manager bietet eine neue Option für AWS WAF Richtlinien. Sie können nun alle vorhandenen Web-ACL-Zuordnungen aus Ressourcen innerhalb des Bereichs entfernen, bevor Sie ihnen die neuen Web-ACLs der Richtlinie zuordnen.	14. Januar 2020
Aktualisierte AWS verwaltete Regeln für AWS WAF	AWS Managed Rules for AWS WAF hat die Texttransformationen für Regeln im Kernregelsatz und in den Regelgruppen der SQL-Datenbank aktualisiert.	20. Dezember 2019

[AWS Firewall Manager
integriert mit AWS Security
Hub](#)

AWS Firewall Manager erstellt jetzt Ergebnisse für Ressourcen, die nicht richtlinientreu sind, und für Angriffe und sendet sie an AWS Security Hub.

18. Dezember 2019

[Veröffentlichung von AWS WAF Version 2](#)

Neue Version des AWS WAF Entwicklerhandbuchs. Sie können eine Web-ACL oder Regelgruppe im JSON-Format verwalten. Zu den erweiterten Funktionen gehören logische Regelanweisungen, Verschachtelung von Regelanweisungen und vollständige CIDR-Unterstützung für IP-Adressen und -Adressbereiche. Regeln sind keine AWS Ressourcen mehr, sondern existieren nur noch im Kontext einer Web-ACL oder Regelgruppe. Für Bestandskunden heißt die vorherige Version des Dienstes jetzt AWS WAF Classic. In den APIs, SDKs und CLIs behält AWS WAF Classic seine Benennungsschemata bei, und diese neueste Version von AWS WAF wird je nach Kontext mit dem Zusatz „V2“ oder „v2“ bezeichnet. AWS WAF kann nicht auf AWS Ressourcen zugreifen, die in Classic erstellt wurden. AWS WAF Um diese Ressourcen in verwenden zu können AWS WAF, müssen Sie sie migrieren.

25. November 2019

AWS Regelgruppen für verwaltete Regeln AWS WAF	Regelgruppen für AWS verwaltete Regeln hinzugefügt. Diese sind für AWS WAF Kunden kostenlos.	25. November 2019
AWS Firewall Manager Unterstützung für Amazon Virtual Private Cloud-Sicherheitsgruppen	Firewall Manager wurde um Unterstützung für Amazon VPC-Sicherheitsgruppen erweitert.	10. Oktober 2019
AWS Firewall Manager Unterstützung für AWS Shield Advanced	Unterstützung für Shield Advanced wurde zu Firewall Manager hinzugefügt.	15. März 2019
Tutorial: Hierarchische Richtlinien erstellen	Zusätzliches Tutorial zum Erstellen hierarchischer Richtlinien in AWS Firewall Manager.	11. Februar 2019
Steuerung auf Regelebene in Regelgruppen	Sie können jetzt einzelne Regeln sowie Ihre eigenen AWS Marketplace Regelgruppen aus Regelgruppen ausschließen.	12. Dezember 2018
AWS Shield Advanced Unterstützung für AWS Global Accelerator Standardbeschleuniger	Shield Advanced kann jetzt AWS Global Accelerator Standardbeschleuniger schützen.	26. November 2018
AWS WAF Unterstützung für Amazon API Gateway	AWS WAF schützt jetzt Amazon API Gateway Gateway-APIs.	25. Oktober 2018

Erweiterter AWS Shield Advanced-Assistent für erste Schritte	Der neue Assistent bietet die Möglichkeit, tarifbasierte Regeln und Amazon CloudWatch Events zu erstellen.	31. August 2018
AWS WAF logging	Aktivieren Sie die Protokollierung, um detaillierte Informationen über den Traffic zu erhalten, der von Ihrer Web-ACL analysiert wird.	31. August 2018
Support für Abfrageparameter in Bedingungen	Beim Erstellen einer Bedingung können Sie jetzt die Anfragen nach bestimmten Parametern durchsuchen.	5. Juni 2018
Shield Advanced Assistent für die ersten Schritte	Führt einen neuen optimierten Prozess für das Abonnieren von AWS Shield Advanced ein.	5. Juni 2018
Erweiterte zulässige CIDR-Bereiche	Beim Erstellen einer IP-Übereinstimmungsbedingung werden AWS WAF jetzt IPv4-Adressbereiche unterstützt: /8 und alle Bereiche zwischen /16 und /32.	5. Juni 2018

Updates vor 2018

In der folgenden Tabelle werden wichtige Änderungen in jeder Version des AWS WAF Entwicklerhandbuchs beschrieben, die vor 2018 vorgenommen wurden.

Änderung	API-Version	Beschreibung	Veröffentlichungsdatum
Aktualisierung	24. August 2016	AWS Marketplace Regelgruppen	November 2017
Aktualisierung	24. August 2016	Shield Advanced-Support für Elastic IP-Adressen	November 2017
Aktualisierung	24. August 2016	Globales Bedrohungs-Dashboard	November 2017
Aktualisierung	24. August 2016	DDoS-resistentes Website-Tutorial	Oktober 2017
Aktualisierung	24. August 2016	Geo- und Regex-Bedingungen	Oktober 2017
Aktualisierung	24. August 2016	Ratenbasierte Regeln	Juni 2017
Aktualisierung	24. August 2016	Reorganisation	April 2017
Aktualisierung	24. August 2016	Zusätzliche Informationen zu DDoS-Schutz und Unterstützung für Application Load Balancer.	November 2016
Neue Features	24. August 2015	Sie können jetzt alle Ihre API-Aufrufe bei AWS WAF through protokollieren AWS CloudTrail, dem AWS Dienst, der API-Aufrufe für Ihr Konto aufzeichnet und Protokolldateien an Ihren S3-Bucket übermittelt. CloudTrail Protokolle können verwendet werden, um Sicherheitsanalysen zu ermöglichen, Änderungen an Ihren AWS Ressourcen nachzuverfolgen und bei der Überprüfung der Einhaltung von Vorschriften zu helfen. Durch die Integration AWS WAF CloudTrail können Sie feststellen, welche Anfragen an die AWS WAF API gestellt wurden, von welcher Quell-IP-Adresse aus	28. April 2016

Änderung	API-Version	Beschreibung	Veröffentlichungsdatum
		<p>jede Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde und vieles mehr.</p> <p>Wenn Sie die API bereits verwenden AWS CloudTrail, werden Ihnen ab sofort AWS WAF API-Aufrufe in Ihrem CloudTrail Protokoll angezeigt. Wenn Sie es CloudTrail für Ihr Konto nicht aktiviert haben, können Sie es über CloudTrail den aktivieren AWS Management Console. Für die Aktivierung fallen keine zusätzlichen Gebühren an CloudTrail, es gelten jedoch Standardtarife für die Nutzung von Amazon S3 und Amazon SNS.</p>	
Neue Features	24. August 2015	<p>Sie können es jetzt verwenden, AWS WAF um Webanfragen zuzulassen, zu blockieren oder zu zählen, die offenbar bössartige Skripts enthalten, was als Cross-Site-Scripting oder XSS bezeichnet wird. Angreifer fügen manchmal schädliche Skripts in Webanforderungen ein, um Schwachstellen in Webanwendungen auszunutzen. Weitere Informationen finden Sie unter Cross-Site-Scripting-Angriffsregel-Anweisung.</p>	29. März 2016

Änderung	API-Version	Beschreibung	Veröffentlichungsdatum
Neue Features	24. August 2015	<p>In dieser Version werden die folgenden AWS WAF Funktionen hinzugefügt:</p> <ul style="list-style-type: none"> • Sie können so konfigurieren AWS WAF , dass Webanfragen auf der Grundlage der Länge bestimmter Teile der Anfragen, wie Abfragezeichenfolgen oder URIs, zugelassen, blockiert oder gezählt werden. Weitere Informationen finden Sie unter Größenbeschränkungsanweisung. • Sie können so konfigurieren AWS WAF , dass Webanfragen auf der Grundlage des Inhalts im Anfragetext zugelassen, blockiert oder gezählt werden. Dies ist der Teil einer Anforderung, der alle zusätzlichen Daten enthält, die Sie als HTTP-Anforderungstext an Ihren Web-Server senden möchten, wie z. B. Formulardaten. Diese Funktion gilt für die Übereinstimmung von Zeichenfolgen, SQL Injections-Übereinstimmungsbedingungen und die neuen Größenbeschränkungsbedingungen, die bereits unter dem ersten Punkt erwähnt wurden. Weitere Informationen finden Sie unter Webanforderungskomponenten. 	27. Januar 2016
Neues Feature	24. August 2015	<p>Sie können jetzt die AWS WAF Konsole verwenden , um die CloudFront Distributionen auszuwählen, denen Sie eine Web-ACL zuordnen möchten. Weitere Informationen finden Sie unter Web-ACL und Distribution zuordnen oder deren Zuordnung aufheben.</p> <p>CloudFront</p>	16. November 2015
Erstversion	24. August 2015	Dies ist die erste Version des AWS WAF -Entwicklerhandbuchs.	6. Oktober 2015

AWS Glossar

Die neueste AWS Terminologie finden Sie im [AWS Glossar](#) in der AWS-Glossar Referenz.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.